Registry System Testing

DNS Test Area Specification

Version B

File name: Test Area DNS.docx
Last saved: 2018-07-19

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 DNS.docx

Revisions

Date	Version	Name	Description
2017-07-27	A	Mats Dufberg	First release version.
2018-07-19	B	Mats Dufberg	All references to DNSCheck or DNSCheck messages removed. Reference to external IANA registry of special purpose IP addresses instead of table of such addresses.

LIST OF CONTENTS

1. Introduction

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

1.1 Scope

The Registry System Testing Provider will test the appointed Registry Service Provider's DNS infrastructure. The Test Cases are performed over IPv4 and IPv6 from five test nodes located in the five ICANN regions.

Those Test Cases labeled "Distributed" use a slightly different methodology and are run from many more test nodes, in order to adequately test anycast DNS clouds. The methodology is described in more detail in section 2.4.1.

1.2 References

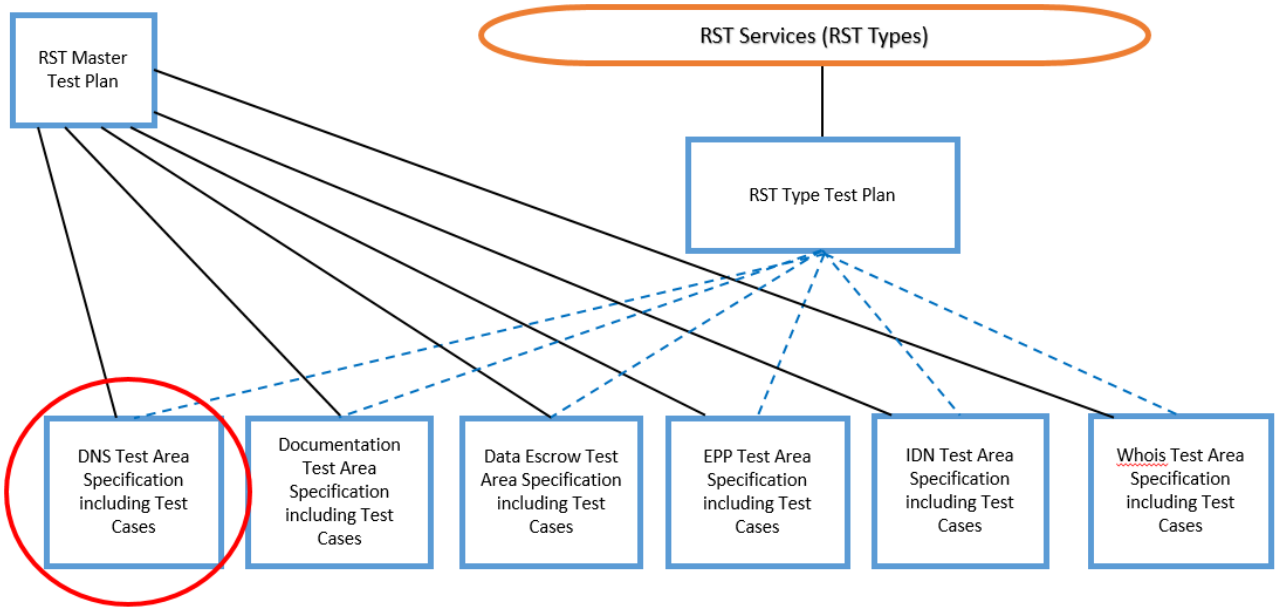
1.2.1 External

- IEEE 829-2008
- ICANN gTLD Applicant Guidebook, Version 2012-06-04
- IANA document "Technical requirements for authoritative name servers"[1]

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] https://www.iana.org/help/nameserver-requirements

1.3 Earlier documents

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

- Pre-Delegation Testing: DNS Test Plan (version H)
- Pre-Delegation Testing: DNS Delegation Test Cases (version K)
- Pre-Delegation Testing: DNS Distributed (version D)
- Pre-Delegation Testing: DNS DNSSEC Test Cases (version H)
- Pre-Delegation Testing: DNS Zone Test Cases (version G)

1.4 Level in the overall sequence

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

1.5 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 Registry Operator provides valid test data.

2. Test Requirements

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 [Registry Operator'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[2]

[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[3]

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 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

[2] Now available as https://www.iana.org/help/nameserver-requirements
[3] Now included in https://www.iana.org/help/nameserver-requirements

- 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. 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 [Registry Operator] and will perform TCP reachability and transaction capability tests across a randomly selected subset of the name servers within the [Registry Operator's] DNS infrastructure. In case of use of anycast, each individual server in each anycast set will be tested.
>
> **DNSSEC support --** [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. In particular, the [Registry Operator] 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 [Registry Operator'] 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 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

2.3 Features not to be tested

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

2.4 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.[4]

All DNS tests that are performed using the DNS protocol on the Registry Service Provider's DNS infrastructure is done from all of the RST Service Provider's testing locations over both 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.

2.4.1 The Distributed Approach

The distributed test cases (DNS16-21 and DNS32-35) are to be performed over IPv4 and IPv6 from many nodes widely distributed over the Internet, where "many" is a lot more than the five nodes in the five different ICANN regions required in the other test cases. The purpose of using many testing nodes is to measure the largest amount of individual anycast locations possible, in order to conclude that the Anycast DNS function is operational.

The number of nodes available for distributed testing vary over time. The current number of nodes that the RST Service Provider can access for distributed tests as of the date of this specification is between 40 and 50, widely distributed globally. The test cases are performed on these nodes using the timeouts and threshold values described below.

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

Availability of a node is based on if the RST Service Provider can connect to the node using SSH, and if it can run the test program without returning any error from the system.

1. If a node does not return answers for all requested queries within **7.5 seconds times the number of queries** (timeout = 7.5s x queries) or if it does not have support to send queries over both IPv4 and IPv6, all data from the node is ignored and the node is disconnected. The node is considered to be **non-available**.
2. The number of nodes available for testing must be **at least 20**.
3. **51% of the available nodes must have a complete set of answers for each query made via the available nodes.** The set of answers from a node is considered complete when **at least 90%** of the queries have **valid DNS responses.**

If the number of available nodes is below the threshold described in 2), a test cannot be performed and the problem must be fixed by the RST Service Provider.

If the number of DNS nodes that have returned a complete set of DNS answers is below the threshold described in 3), all distributed test cases fail.

2.5 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.

2.6 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 Registry Operator or the RST tester.

2.7 Test deliverables

The DNS test level will produce:

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

3. Test Traceability Matrix

This table describes the different test cases and their mapping to the requirements.

Test ID	Test Group	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

Test ID	Test Group	Description	Requirement Point
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
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
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
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

Test ID	Test Group	Description	Requirement Point
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
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
DNS36 RRSIG(SOA) must validate with supplied DS record	DNSSEC	The DS record supplied must have a working chain-of-trust down to the signature over the SOA record.	R25, R28, DS2

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 DNS01: Minimum number of name servers (Delegation)

5.1 Test case identifier

DNS01

5.2 Objective

There must be at least two NS records listed in a delegation, and the hosts must not resolve to the same IP address.

This test case fulfills the requirement in the "Technical requirements for authoritative name servers"[5] document referenced in 2.1.1.

5.3 Inputs

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

Id	Description	Type
TLD	The ASCII compatible name of the TLD	String
DnsNameServer-[1..n]	FQDN of authoritative name server	String
DnsGlueRecord-[1..n]	All IPv4 or IPv6 addresses for auth NS	String

The above input is also considered to be the exact same information that is sent to IANA for inclusion in the root zone. IANA will only publish the subordinate host glue records in the root zone.

5.4 Outcome(s)

There must be at least two name servers in the input delegation data. If there are less than two distinct IPv4 addresses for the delegated name servers this test case fails.

There must be at least two distinct IPv6 addresses for the delegated name servers. If there are less than two distinct IPv6 addresses this test case fails.

There must be at least two NS records for the delegation. If there are less than two NS this test case fails.

5.5 Environmental needs

All authoritative name servers listed in the inputs section 5.3 should be authoritative for the designated zone.

5.6 Special procedural requirements

This test has no procedural requirements.

5.7 Intercase dependencies

This test has no intercase dependencies.

[5] https://www.iana.org/help/nameserver-requirements

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

An NS query is made to all listed name servers for the designated zone. The NS records in the answer are compared with the parent zone (from the input data). If the total number of common NS records between parent and zone is less than two a message is generated.

The IP addresses of all NS records are collected. If the total count of distinct IPv4 addresses is below 2 a message is generated. If the total count of distinct IPv6 addresses is below 2 a message is generated. If the total of common NS records in the delegation from both the parent and the child zone is below 2, a message is also generated.

6. Test Case DNS02: Name server reachability (Delegation)

6.1 Test case identifier

DNS02

6.2 Objective

The name servers must answer DNS queries over both the UDP and TCP protocols on port 53.

This test case fulfills the requirements 2.3.1 in the "Technical requirements for authoritative name servers"[6] document, and the requirements on TCP and UDP of section 5.2 in the Applicant Guidebook.

6.3 Inputs

See section 5.3 in this document.

6.4 Outcome(s)

If any query is failing to get an answer, an error message is generated and this test case fails.

6.5 Environmental needs

All authoritative name servers listed in the inputs section 5.3 must be authoritative for the designated zone.

6.6 Special procedural requirements

This test has no procedural requirements.

6.7 Intercase dependencies

This test has no intercase dependencies.

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

A SOA query is sent over UDP and TCP to all the listed nameservers. If any query fails to give an answer, a message is generated.

[6] https://www.iana.org/help/nameserver-requirements

7. Test Case DNS03: Answer authoritatively (Delegation)

7.1 Test case identifier

DNS03

7.2 Objective

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.

This test case fulfills the requirements 2.4.1 and 2.4.2 in the "Technical requirements for authoritative name servers"[7] document.

7.3 Inputs

See section 5.3 in this document.

7.4 Outcome(s)

If any name server answers without the AA-bit, an error message is generated and this test case fails.

7.5 Environmental needs

All authoritative name servers listed in the inputs section 5.3 should be authoritative for the designated zone.

7.6 Special procedural requirements

This test has no procedural requirements.

7.7 Intercase dependencies

This test has no intercase dependencies.

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

All listed name servers are queried for the SOA record over UDP and TCP. If any of the name servers fail to give an authoritative answer ("AA-bit" is set in the answer), a message is generated.

[7] https://www.iana.org/help/nameserver-requirements

8. Test Case DNS04: Network diversity (Delegation)

8.1 Test case identifier

DNS04

8.2 Objective

The name servers must be in at least two topologically separate networks for IPv4 and IPv6, respectively.

This test case fulfills the requirements 2.5.2 in the "Technical requirements for authoritative name servers"[8] document.

8.3 Inputs

See section 5.3 in this document. In addition to this we use the IP to ASN mapping in the RIPE RIS database[9].

8.4 Outcome(s)

There must be at least two different origin ASs from the process described in section 8.8. The RIPE RIS database is used to determine if at least two origin ASs are used. If it does not report at least two origin ASs for IPv4 and IPv6, respectively, this test case fails. The two origin ASs must also have some independence as described in the steps below.

8.5 Environmental needs

The RIPE RIS database must be available online.

8.6 Special procedural requirements

This test has no procedural requirements.

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. All NS records and their IP addresses are looked up for the designated zone.
2. The following steps are done independently for the IPv4 and IPv6 addresses, respectively, and both protocols must pass.
    a. For all IP addresses do a lookup of origin ASNs using one of the following commands[10]:
    whois -h riswhois.ripe.net -- "-F -M **<IPaddr>**"
    whois -h riswhois.ripe.net -- "-M **<IPaddr>**"
    b. Each lookup will result in a set of origin ASNs (one or more ASNs). Save that set to a list of sets.
    c. When comparing two sets in the list, the sets are considered to be equal if they have the same ASNs as elements. The order between ASNs in a set shall be ignored.

[8] https://www.iana.org/help/nameserver-requirements
[9] http://www.ripe.net/data-tools/stats/ris/routing-information-service
[10] The exact command can vary depending on OS on which the command is executed. The example here is from a computer with Ubuntu Linux. Also see http://www.ripe.net/ris/riswhois.html

d. Compare the sets in the list. If there are two sets in the lists thar are NOT equal, then the tested protocol (IPv4 or IPv6) will pass, or else it will fail.

3. If both IPv4 and IPv6 pass the steps above, this Test Cass ends with PASS, else it ends with FAIL.

8.9 Examples of passing and failing configurations

In our examples the nameservers have three IP addresses, x_1, x_2 and x_3. The lookup of origin gives the result as below.

Example 1. This configuration is a PASS. Two addresses have different origin ASs:

x_1: 65536
x_2: 65536, 65550
x_3: 65550

Example 2. This configuration is also a PASS. One address has a different configuration of origin ASs than the other:

x_1: 65536
x_2: 65536, 65550
x_3: 65536, 65550

Example 3. This configuration is a FAIL. All addresses have the same configuration of origin ASs:

x_1: 65536, 65550
x_2: 65536, 65550
x_3: 65536, 65550

Example 3. This configuration is also a FAIL. The addresses have only one and the same origin AS:

x_1: 65536
x_2: 65536
x_3: 65536

Note that the tests of origin ASs are done independently on IPv4 and IPv6, and that both must meet the requirements to give a PASS on this test case.

9. Test Case DNS05: Consistency between glue and authoritative data (Delegation)

9.1 Test case identifier

DNS05

9.2 Objective

For name servers that have IP addresses listed as glue, the IP addresses must match the authoritative A and AAAA records for that host.

This test case fulfills the requirements 2.6.1 in the "Technical requirements for authoritative name servers"[11] document.

9.3 Inputs

See section 5.3 in this document.

9.4 Outcome(s)

If there is an inconsistency between the IP-addresses for any host on any authoritative name server, an error message is generated and this test case fails.

9.5 Environmental needs

All authoritative name servers listed in the inputs section 5.3 should be authoritative for the designated zone.

9.6 Special procedural requirements

This test has no procedural requirements.

9.7 Intercase dependencies

This test has no intercase dependencies.

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

The name server data on the input parameters side is compared to the content of the answers for all the name servers. If there is an inconsistency between the sets of IP-addresses a message is generated.

[11] https://www.iana.org/help/nameserver-requirements

10. Test Case DNS06: Consistency between delegation and zone (Delegation)

10.1 Test case identifier

DNS06

10.2 Objective

The set of NS records served by the authoritative name servers must match those proposed for the delegation in the parent zone.

This test case fulfills the requirements 2.7.1 in the "Technical requirements for authoritative name servers"[12] document.

10.3 Inputs

See section 5.3 in this document.

10.4 Outcome(s)

The NS sets between the parent and the child zone must be consistent. If the NS sets are not consistent an error message is generated and this test case fails.

10.5 Environmental needs

All authoritative name servers listed in the inputs section 5.3 should be authoritative for the designated zone.

10.6 Special procedural requirements

This test has no procedural requirements.

10.7 Intercase dependencies

This test has no intercase dependencies.

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

All authoritative name servers are queried for the NS set. The name server data on the input parameters side is compared to the content of the answers for all the name servers. If there is an inconsistency between the NS record sets, a message is generated.

[12] https://www.iana.org/help/nameserver-requirements

11. Test Case DNS07: SOA record consistency between authoritative name servers (Delegation)

11.1 Test case identifier

DNS07

11.2 Objective

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 zone.

This test case fulfills the requirements 2.8.1 and 2.8.3 in the "Technical requirements for authoritative name servers" document.

11.3 Inputs

See section 5.3 in this document.

11.4 Outcome(s)

All authoritative name servers must have consistent SOA digests and SOA serial values. If there is any inconsistency, an error messages is generated, and this test case fails in this first step.

If there are occurrences of the error, there is a manual inspection of the SOA Serial numbers in the logs. See the requirement in 2.8.3.1 in the "Technical requirements for authoritative name servers"[13] document. If the difference of the SOA Serial is considered minor, the error is discarded, and the test case is passed. If the difference is considered major, this test case fails.

11.5 Environmental needs

All name servers listed in the inputs section 5.3 should be authoritative for the designated zone.

11.6 Special procedural requirements

If for operational reasons the zone content fluctuates rapidly, the serial numbers need only be loosely coherent.

There are several different methods to set the SOA Serial number. The most popular are "unix time" where the Serial is a second counter based on unix time, "date" where the Serial is a date and a serial number counter at the end, and "counter" where the Serial value is just any type of counter. The most common use is probably "unix time". In both "date" and "unix time" it should be easy to note that the authoritative name servers do not differ any more than a few serial number updates. A manual inspection of the SOA serial should be enough to determine if the zone updates work properly or not, and if the serial values are within a reasonable range, the test is ok.

11.7 Intercase dependencies

This test has no intercase dependencies.

[13] https://www.iana.org/help/nameserver-requirements

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

The SOA record is queried from all the name servers found in the input parameters, and also in the zone itself. If the SOA serial number is not all the same for all the answers, a message is generated. A digest is calculated from the SOA records as well, and if the digest is not all the same for all the answers a message is generated.

12. Test Case DNS08: NS record consistency between authoritative name servers (Delegation)

12.1 Test case identifier

DNS08

12.2 Objective

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 zone domain.

This test case fulfills the requirements 2.8.1 and 2.8.2 in the "Technical requirements for authoritative name servers"[14] document.

12.3 Inputs

See section 5.3 in this document.

12.4 Outcome(s)

All authoritative name servers must have consistent NS sets in the answer. If there is any inconsistency in the answers, a message is generated and this test case fails.

12.5 Environmental needs

All authoritative name servers listed in the inputs section 5.3 should be authoritative for the designated zone.

12.6 Special procedural requirements

This test has no procedural requirements.

12.7 Intercase dependencies

This test has no intercase dependencies.

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

An NS record query for the TLD is made for all the name servers found in the input parameters. If any of the NS records in an authoritative answer is not consistent with any of the other answers, a message is generated.

[14] https://www.iana.org/help/nameserver-requirements

13. Test Case DNS09: No truncation of referrals (Delegation)

13.1 Test case identifier

DNS09

13.2 Objective

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.

This test case fulfills the requirements 2.9.1 and 2.9.2 in the "Technical requirements for authoritative name servers" document.

13.3 Inputs

See section 5.3 in this document.

13.4 Outcome(s)

The created DNS referral packet must not be more than 512 octets. If the DNS packet is larger than 512 bytes, a message is generated and this test case fails.

13.5 Environmental needs

This test has no environmental requirements.

13.6 Special procedural requirements

This test has no procedural requirements.

13.7 Intercase dependencies

This test has no intercase dependencies.

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

An empty DNS answer packet is generated. All NS records from the input, and all the in-bailiwick glue is added to the packet. If the size of the packet is more than 512 octets a message is generated.

14. Test Case DNS10: Prohibited networks (Delegation)

14.1 Test case identifier

DNS10

14.2 Objective

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.[15]

This test case fulfills the requirements in 2.10 of the "Technical requirements for authoritative name servers"[16] document.

14.3 Inputs

See section 5.3 in this document.

14.4 Outcome(s)

All IP addresses used by the name servers in the delegation for the designated zone must be globally routable. If any of the IP addresses used is reserved, private or otherwise unsuitable (see the table in 14.8), an error messages is generated and this test case fails.

14.5 Environmental needs

This test has no environmental requirements.

14.6 Special procedural requirements

This test has no procedural requirements.

14.7 Intercase dependencies

This test has no intercase dependencies.

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

All name servers found in the input parameters are queried for their IP addresses in the zone. Along with IP addresses from the input data, all addresses are is compared to a list containing blocks of reserved IPv4 addresses not suitable for global routing, blocks of reserved IPv6 addresses not suitable for global routing, and Teredo and 6to4 IPv6 tunnel addresses.

For IPv4 addresses the *IANA IPv4 Special-Purpose Address Registry* is used:

- https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml

For IPv6 addresses the *IANA IPv6 Special-Purpose Address Registry* is used:

- https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

,

[15] See https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml and https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

[16] https://www.iana.org/help/nameserver-requirements

15. Test Case DNS11: No open recursive name service (Delegation)

15.1 Test case identifier

DNS11

15.2 Objective

The authoritative name servers must not provide recursive name service.

This test case fulfills the requirements 2.11.1 in the "Technical requirements for authoritative name servers"[17] document.

15.3 Inputs

See section 5.3 in this document.

15.4 Outcome(s)

No name server must respond with a possible referral packet. If the response is a referral, a message is generated and this test case fails.

15.5 Environmental needs

All authoritative name servers listed in the inputs section 5.3 should be authoritative for the designated zone.

15.6 Special procedural requirements

This test has no procedural requirements.

15.7 Intercase dependencies

This test has no intercase dependencies.

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

A SOA query for an almost certainly nonexistent name sent to the list of name servers, with the recursion request and DNSSEC flags set, resulting in a response with the recursion available flag set, an RCODE other than SERVFAIL or REFUSED and not referring to other servers. If the response is a possible referral, a message is generated.

[17] https://www.iana.org/help/nameserver-requirements

16. Test Case DNS12: Same source address (Delegation)

16.1 Test case identifier

DNS12

16.2 Objective

Responses from the authoritative name servers must contain the same source IP address as the destination IP address of the initial query.

This test case fulfills the requirements 2.12.1 in the "Technical requirements for authoritative name servers"[18] document.

16.3 Inputs

See section 5.3 in this document.

16.4 Outcome(s)

The DNS answer must come from the same source IP address as the destination of the query. If there is a mismatch, a message is generated and this test case fails.

16.5 Environmental needs

All authoritative name servers listed in the inputs section 5.3 should be authoritative for the designated zone.

16.6 Special procedural requirements

This test has no procedural requirements.

16.7 Intercase dependencies

This test has no intercase dependencies.

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

One query per authoritative name server IP address is made, and the answer is verified to come from the same IP address. If there is a mismatch between these IP addresses, a message is generated.

[18] https://www.iana.org/help/nameserver-requirements

17. Test Case DNS14: Legal values for the DS hash digest algorithm (DNSSEC)

17.1 Test case identifier

DNS14

17.2 Objective

For the hash digest, ICANN supports two types — SHA1 (value 1), and SHA256 (value 2). The DnsKeyDigestType for the supplied DS records must match one of those type values.

This test case fulfills the DNSSEC and Anycast requirements 5.2.2 in the gTLD Application Handbook, Module 5 and the tests described in the "Technical requirements for authoritative name servers"[19] document.

17.3 Inputs

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

Id	Description	Type
TLD	The ASCII compatible name of the TLD	String
DnsKeyDigest-[1..n]	The digest (DS) of the DNSKEY	String
DnsKeyTag-[1..n]	The key tag of the DNSKEY	Number
DnsKeyAlgorithm-[1..n]	The algorithm number of the DNSKEY	Number
DnsKeyDigestType-[1..n]	The digest type number of the DS	Number
DnsNameServer-[1..n]	FQDN of authoritative name server	String
DnsGlueRecord-[1..n]	All IPv4 or IPv6 addresses for auth NS	String

The above input parameters are not the name server delegation data, but the name of the designated zone and a list of DS records that is to be published in the root zone.

17.4 Outcome(s)

All submitted DS records must have a valid DS hash algorithm digest type; the value must be either 1 or 2. (There are more valid DS hash algorithms, but these are not at the moment allowed for publication in the root zone.)

17.5 Environmental needs

This test has no environmental needs.

17.6 Special procedural requirements

This test has no special procedural requirements.

17.7 Intercase dependencies

This test has no intercase dependencies.

[19] https://www.iana.org/help/nameserver-requirements

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

The test program is executed with all of the input parameters described in section 17.3. The DnsKeyDigestType input number is compared with the values 1 and 2, where it must match either.

18. Test Case DNS15: DS must match a DNSKEY in the designated zone (DNSSEC)

18.1 Test case identifier

DNS15

18.2 Objective

There must be a DNSKEY that matches the DS record present in the child zone.

This test case fulfills the anycast requirements 5.2.2 in the gTLD Application Handbook, Module 5 and the tests described in the "Technical requirements for authoritative name servers"[20] document.

18.3 Inputs

See section 17.3 for all input parameters.

18.4 Outcome(s)

All submitted DS records must match a DNSKEY that is published on all the authoritative name servers for the designated zone, or else the test will emit a failure. If the matched DNSKEY is a ZSK, and not a KSK, then a warning will be emitted.

18.5 Environmental needs

All authoritative name servers listed in the inputs section 17.3 should be authoritative for the designated zone.

18.6 Special procedural requirements

If a top-level domain operator has a situation where all DS records does not match a DNSKEY, and this is by design and can be demonstrated not to affect the stability of the TLD or the root zone, it is possible to request that the DS records be "listed" regardless. This test case will give a notify message as the result of the test after discussing with the domain operator.

(Note: At least one DS must always match a DNSKEY.)

This is the same procedure as for the final publication of the DS records in the root zone.

18.7 Intercase dependencies

This test has no intercase dependencies.

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

The test program is executed with all of the input parameters described in section 17.3.

For each DS record from the input parameters do:

- Send a query for DNSKEY to all specified authoritative name servers.
- Verify that there is a matching DNSKEY in the answer section for all queries made.
- If a matching DNSKEY does not have the Secure Entry Point flag set, emit a warning.

[20] https://www.iana.org/help/nameserver-requirements

19. Test Case DNS16: Signatures in the designated zone must validate (Distributed)

19.1 Test case identifier

DNS16

19.2 Objective

Verify that the provided DNSSEC trust anchor can be used to validate DNSSEC signatures (RRSIG) in the test zone.

This test case fulfills the DNSSEC validation requirement R25 from the Statement of Work.

19.3 Inputs

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

Id	Description	Type
TLD	The ASCII compatible name of the TLD	String
DnsKeyDigest-[1..n]	The digest (DS) of the DNSKEY	String
DnsKeyTag-[1..n]	The key tag of the DNSKEY	Number
DnsKeyAlgorithm-[1..n]	The algorithm number of the DNSKEY	Number
DnsKeyDigestType-[1..n]	The digest type number of the DS	Number
DnsNameServer-[1..n]	FQDN of authoritative name server	String
DnsGlueRecord-[1..n]	All IPv4 or IPv6 addresses for auth NS	String
SubDomain	A delegated domain with NS and DS records published in the TLD zone	String

The above input is also considered to be the exact same information that is sent to IANA for inclusion in the root zone, except for the SubDomain. IANA will only publish the subordinate host glue records in the root zone.

19.4 Outcome(s)

After the measurement criteria in section 2.4.1 has been passed, the following outcome must be true for all DNS answers, or this test case fails:

- The signatures covering the DNSKEY record must be validated following the DNSSEC chain from the given DS records.
- The signatures covering the SOA record must be validated following the DNSSEC chain from the given DS records.

19.5 Environmental needs

All authoritative name servers listed in the inputs section 19.3 should be authoritative for the designated zone.

The node availability criteria described in section 2.4.1 also apply to this test.

19.6 Special procedural requirements

This test has no special procedural requirements.

19.7 Intercase dependencies

This test has no intercase dependencies.

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

The test program is executed with all of the input parameters described in section 19.3.

For each name server, a query is sent to all the name servers for the DNSKEY record. The answers must contain DNSKEY records and an RRSIG record(s). The signature is validated with the DNSKEYs found, and then matched with the DS record from the input.

For each unique DNSKEY algorithm found in the, there must be an RRSIG matching each algorithm.

20. Test Case DNS17: Zone contains NSEC or NSEC3 records (Distributed)

20.1 Test case identifier

DNS17

20.2 Objective

Verify that correct NSEC or NSEC3 records with valid signatures are returned for a query for an non-existent name.

This test case fulfills the DNSSEC validation requirement AGB3 from the Applicant Guidebook.

20.3 Inputs

See section 19.3 for all input parameters.

20.4 Outcome(s)

After the measurement criteria in section 2.4.1 has been passed, the following outcome must be true for all DNS answers, or this test case fails:

The signatures covering the NSEC or NSEC3 record must be validated following the DNSSEC chain from the given DS records. If the records are not present, if the records are not correct or if an invalid RRSIG is returned, this test fails.

20.5 Environmental needs

All authoritative name servers listed in the inputs section 19.3 should be authoritative for the designated zone.

The node availability criteria described in section 2.4.1 also apply to this test.

20.6 Special procedural requirements

This test has no special procedural requirements.

20.7 Intercase dependencies

This test has no intercase dependencies.

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

The test program is executed with all of the input parameters described in section 19.3.

A query is made for the SOA record on xx--example.[TLD], a label that should never occur because of the prefix. The answer should contain correct NSEC or NSEC3 records (according to the DNSSEC standards) with valid signatures.

21. Test Case DNS18: Consistency between glue and authoritative data (Distributed)

21.1 Test case identifier

DNS18

21.2 Objective

For name servers that have IP addresses listed as glue, the IP addresses must match the authoritative A and AAAA records for that host.

21.3 Inputs

See section 19.3 for all input parameters.

21.4 Outcome(s)

After the measurement criteria in section 2.4.1 has been passed, the following outcome must be true for all DNS answers, or this test case fails:

This test fails if there is a glue record (A or AAAA) in the delegation that does not exist in the delegated zone, i.e. the owner name and IP address of the record must be the same.

21.5 Environmental needs

All authoritative name servers listed in the inputs section 19.3 must be authoritative for the designated zone.

The node availability criteria described in section 2.4.1 also apply to this test.

21.6 Special procedural requirements

This test case is dependent on the availability of all unicast addresses, however we cannot verify that all unicast addresses has been made available for testing.

21.7 Intercase dependencies

This test has no intercase dependencies.

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

For each name server in the input parameter (DnsNameServer) send a DNS query for each glue record. Compare the RR set in the response with the glue record. If there is no record in the answer with the same owner name and IP address as the glue record, the entire test fails. The RR set may contain additional records."

22. Test Case DNS19: SOA record consistency between authoritative name servers (Distributed)

22.1 Test case identifier

DNS19

22.2 Objective

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 zone.

22.3 Inputs

See section 19.3 in this document.

22.4 Outcome(s)

After the measurement criteria in section 2.4.1 has been passed, the following outcome must be true for all DNS answers, or this test case fails:

If there is an inconsistency between any SOA records retrieved for the designated zone, the test fails.

If there are occurrences of different SOA Serial numbers, we manually inspect the Serial numbers in the logs. See the requirement in 2.8.3.1 in the "Technical requirements for authoritative name servers"[21] document.

22.5 Environmental needs

All authoritative name servers listed in the inputs section 19.3 must be authoritative for the designated zone.

The node availability criteria described in section 2.4.1 also apply to this test.

22.6 Special procedural requirements

If for operational reasons the zone content fluctuates rapidly, the serial numbers need only be loosely coherent. Manual inspection of the logs is performed in case of the occurrence of different SOA Serial numbers.

There are several different methods to set the SOA Serial number. The most popular are "unix time" where the Serial is a second counter based on unix time, "date" where the Serial is a date and a serial number counter at the end, and "counter" where the Serial value is just any type of counter. The most common use is probably "unix time". In both "date" and "unix time" it should be easy to note that the name servers do not differ any more than a few serial number updates. A manual inspection of the SOA serial should be enough to make a decision on whether the name server updates work properly or not, and if the serial values are within a reasonable range the test is ok.

22.7 Intercase dependencies

This test has no intercase dependencies.

[21] https://www.iana.org/help/nameserver-requirements

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

A SOA query for the designated zone is made for each name server in the input data described in section 19.3. If the answers are not consistent this test fails.

23. Test Case DNS20: NS record consistency between authoritative name servers (Distributed)

23.1 Test case identifier

DNS20

23.2 Objective

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 zone.

23.3 Inputs

See section 19.3 in this document.

23.4 Outcome(s)

After the measurement criteria in section 2.4.1 has been passed, the following outcome must be true for all DNS answers, or this test case fails:

If there is an inconsistency between any set of NS records retrieved for the designated zone, the test fails.

23.5 Environmental needs

All authoritative name servers listed in the inputs section 19.3 must be authoritative for the designated zone.

The node availability criteria described in section 2.4.1 also apply to this test.

23.6 Special procedural requirements

This test case is dependent on the availability of all unicast addresses, however we cannot verify that all unicast addresses has been made available for testing.

23.7 Intercase dependencies

This test has no intercase dependencies.

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

An NS query for the designated zone is made for each name server in the input data described in section 19.3. If the answers are not consistent this test fails.

24. Test Case DNS21: No open recursive name service (Distributed)

24.1 Test case identifier

DNS21

24.2 Objective

The authoritative name servers must not provide recursive name service.

24.3 Inputs

See section 19.3 in this document.

24.4 Outcome(s)

After the measurement criteria in section 2.4.1 has been passed, the following outcome must be true for all DNS answers, or this test case fails:

If any of the authoritative name servers returns with an RCODE other than SERVFAIL or REFUSED, this test case fails.

24.5 Environmental needs

All authoritative name servers listed in the inputs section 19.3 must be authoritative for the designated zone.

The node availability criteria described in section 2.4.1 also apply to this test.

24.6 Special procedural requirements

This test case is dependent on the availability of all unicast addresses; however, we cannot verify that all unicast addresses has been made available for testing.

24.7 Intercase dependencies

This test has no intercase dependencies.

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

A SOA query for an almost certainly nonexistent name (e.g., example.com) is sent to the list of name servers, with the recursion request and DNSSEC flags set, resulting in a response with the recursion available flag set, an RCODE other than SERVFAIL or REFUSED and not referring to other servers. If the response is a possible referral, a failure message is emitted from the test of the name server.

25. Test Case DNS23: Check invalid syntax for SOA RNAME (Delegation)

25.1 Test case identifier

DNS23

25.2 Objective

The SOA RNAME field must be valid in accordance with section 3.3.13 in RFC 1035 and section 3.4 in RFC 2822.

This test case is an addition to the Statement of Work; see section 2.1.2.

25.3 Inputs

See section 5.3 in this document.

25.4 Outcome(s)

The SOA field RNAME must comply with RFC 2822 "Address Specification". If the validation of RNAME fails, a message is generated and this test case fails.

25.5 Environmental needs

This test has no environmental requirements.

25.6 Special procedural requirements

This test has no procedural requirements.

25.7 Intercase dependencies

This test has no intercase dependencies.

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

A SOA query is made to all authoritative name servers. The SOA field RNAME is validated against the rules described in RFC 2822, "Address Specification". If the RNAME field does not validate, a message is generated.

26. Test Case DNS24: SOA Minimum (Delegation)

26.1 Test case identifier

DNS24

26.2 Objective

The SOA Minimum field must be set to 300 seconds or more.

This test case is an addition to the Statement of Work; see section 2.1.2.

26.3 Inputs

See section 5.3 in this document.

26.4 Outcome(s)

The SOA Minimum value must not be less than 300. If the value is less than 300, a message is returned and this test case emits a warning.

26.5 Environmental needs

This test has no environmental requirements.

26.6 Special procedural requirements

This test has no procedural requirements.

26.7 Intercase dependencies

This test has no intercase dependencies.

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

The value from the SOA Minimum field is retrieved. If the value is less than 300 a message is generated.

27. Test Case DNS25: NSEC3 iterations (DNSSEC)

27.1 Test case identifier

DNS25

27.2 Objective

The number of NSEC3 Iterations must meet the requirements of RFC 5155, section 10.3 and RFC 6781, section 5.3.2.

This test case is an addition to the Statement of Work; see section 2.1.2.

27.3 Inputs

See section 17.3 in this document.

27.4 Outcome(s)

If the NSEC3 Iterations value is greater than 100 this test emits a warning (RFC 6781). If the NSEC3 Iterations is greater what is stated in RFC 5155 (section 10.3), depending on key size, then this test emits a failure. The limits for failure are based on the size of the smallest key, rounded up to the nearest table value or rounded down if the key is larger than the largest table value (table from RFC 5155):

Key size	**Iterations**
1024	150
2048	500
4096	2500

27.5 Environmental needs

This test has no environmental requirements.

27.6 Special procedural requirements

This test has no procedural requirements.

27.7 Intercase dependencies

This test has no intercase dependencies.

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

The test program is executed with all of the input parameters described in section 17.3.

1. The Iterations value from the NSEC3PARAM is retrieved from all specified authoritative name servers.
2. The DNSKEY set is retrieved, and the smallest key size is selected.
3. The number of iterations is compared to the value 100.
4. If the number is higher than 100, it is compared to the values stated in RFC 5155 (see table above).

28. Test Case DNS26: RRSIG lifetimes (DNSSEC)

28.1 Test case identifier

DNS26

28.2 Objective

Check that RRSIG lifetimes are not too short (12 hours) or too long (180 days).

This test case is an addition to the Statement of Work; see section 2.1.2.

28.3 Inputs

See section 17.3 for all input parameters.

28.4 Outcome(s)

If any of the RRSIG lifetimes are lower than 12 hours or higher than 180 days, the test emits a warning.

28.5 Environmental needs

All authoritative name servers listed in the inputs section 17.3 should be authoritative for the designated zone.

28.6 Special procedural requirements

This test has no special procedural requirements.

28.7 Intercase dependencies

This test has no intercase dependencies.

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

The test program is executed with all of the input parameters described in section 17.3.

The RRSIG records are retrieved. The signature lifetimes covering the DNSKEY and the SOA records are then matched against the lower value of 12 hours and the upper value 180 days, and if the lifetimes are out of this range the test emits a warning.

29. Test Case DSN27: DNSKEY algorithms (DNSSEC)

29.1 Test case identifier

DNS27

29.2 Objective

Check that there are no invalid DNSKEY algorithms used by any DNSKEY in the designated zone.

This test case is an addition to the Statement of Work; see section 2.1.2.

29.3 Inputs

See section 17.3 for all input parameters.

29.4 Outcome(s)

If any of the DNSKEY algorithm numbers does not match the IANA defined DNSKEY algorithm types, the test emits a warning.

29.5 Environmental needs

All authoritative name servers listed in the inputs section 17.3 should be authoritative for the designated zone.

29.6 Special procedural requirements

This test has no special procedural requirements.

29.7 Intercase dependencies

This test has no intercase dependencies.

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

The test program is executed with all of the input parameters described in section 17.3.

All DNSKEY records are retrieved from the designated zone. The DNSKEY algorithm number is derived from the DNSKEY record and compared to the list of valid DNSKEY algorithms as defined by IANA.[22]

[22] http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml

30. Test Case DNS28: TTL on DS records (Zone)

30.1 Test case identifier

DNS28

30.2 Objective

The TTL on DS records in the designated zone must not be too long (>172800 seconds).

30.3 Inputs

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

Id	Description	Type
TLD	The ASCII compatible name of the TLD	String
DnsNameServer-[1..n]	FQDN of authoritative name server	String
DnsGlueRecord-[1..n]	All IPv4 or IPv6 addresses for auth NS	String
SubDomain	A delegated domain with NS and DS records published in the TLD zone	String

The above input is also considered to be the exact same information that is sent to IANA for inclusion in the root zone. IANA will only publish the subordinate host glue records in the root zone.

30.4 Outcome(s)

All TTL values from the DS record must be less than or equal to 172800 seconds for this test to pass. If there are missing DS records, or the TTL value is higher than 172800 this test emits a warning.

30.5 Environmental needs

All authoritative name servers listed in the inputs section should be authoritative for the designated zone.

30.6 Special procedural requirements

This test has no procedural requirements.

30.7 Intercase dependencies

This test has no procedural requirements.

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

A query for the DS record of the SubDomain is done for all the listed name servers. The TTL of the DS record is evaluated, and it must not exceed 172800 seconds.

31. Test Case DNS29: Wildcards (Zone)

31.1 Test case identifier

DNS29

31.2 Objective

There must not be any wildcards in the designated zone.

31.3 Inputs

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

Id	Description	Type
TLD	The ASCII compatible name of the TLD	String
DnsNameServer-[1..n]	FQDN of authoritative name server	String
DnsGlueRecord-[1..n]	All IPv4 or IPv6 addresses for auth NS	String

The above input is also considered to be the exact same information that is sent to IANA for inclusion in the root zone. IANA will only publish the subordinate host glue records in the root zone.

31.4 Outcome(s)

Both queries must answer with the RCODE NXDOMAIN for this test to pass. All other RCODEs will generate a fail.

31.5 Environmental needs

All authoritative name servers listed in the inputs section should be authoritative for the designated zone.

31.6 Special procedural requirements

This test has no procedural requirements.

31.7 Intercase dependencies

This test has no procedural requirements.

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

Two queries are made, for the A and the AAAA records for an almost certainly nonexistent name in the designated zone. The RCODE should not be NOERROR.

32. Test Case DNS30: Dotless domain (Zone)

32.1 Test case identifier

DNS30

32.2 Objective

The apex of the domain must not contain authoritative data such as an A/AAAA record, or an MX record, for use as what is called a ”dotless domain”.

32.3 Inputs

See section 31.3 in this document.

32.4 Outcome(s)

All queries must answer with the RCODE NOERROR, and the ANSWER and AUTHORITY parts of the answer must not contain NS records for this test to pass. Any NS records in the answer will fail this test.

32.5 Environmental needs

All authoritative name servers listed in the inputs section should be authoritative for the designated zone.

32.6 Special procedural requirements

This test has no procedural requirements.

32.7 Intercase dependencies

This test depends on the EPP test level to finish, since we need a registered domain with a secure delegation in order to have a DS record available for testing.

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

Three queries are made, for the A, the AAAA and the MX records for the label <TLD> in the designated zone. The RCODE should be NOERROR, with the ANSWER and AUTHORITY parts of the answer should be empty.

33. Test Case DNS31: nic.<TLD> or whois.nic.<TLD> must be delegated (Zone)

33.1 Test case identifier

DNS31

33.2 Objective

The names nic.<TLD> or whois.nic.<TLD> must be a delegated zone.

33.3 Inputs

See section 31.3 in this document.

33.4 Outcome(s)

The answer must be NOERROR and the ANSWER or AUTHORITY section must contain NS records, for either nic.<TLD> or whois.nic.<TLD>. If any of the queries fail to return an NS set, this test fails.

33.5 Environmental needs

All authoritative name servers listed in the inputs section should be authoritative for the designated zone.

33.6 Special procedural requirements

This test has no procedural requirements.

33.7 Intercase dependencies

This test depends on the EPP test level to finish, since we need a registered domain with a secure delegation in order to have a DS record available for testing.

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

A query is made for the NS record for the label nic.<TLD> and the whois.nic.<TLD> in the designated zone. The answer should be a set of NS records for the name server handling the delegation.

34. Test Case DNS32: Name server reachability (Distributed)

34.1 Test case identifier

DNS32

34.2 Objective

The name servers must answer DNS queries over both the UDP and TCP protocols on port 53.

This test case fulfills the requirements 2.3.1 in the "Technical requirements for authoritative name servers"[23] document, and the requirements on TCP and UDP of section 5.2 in the Applicant Guidebook.

34.3 Inputs

See section 19.3 in this document.

34.4 Outcome(s)

After the measurement criteria in section 2.4.1 has been passed, the following outcome must be true for all DNS answers, or this test case fails:

All name servers answers over UDP and TCP. If any of the listed name servers in section 19.3 does not answer below the threshold level described below this paragraph, this test case fails.

34.5 Environmental needs

All authoritative name servers listed in the inputs section 19.3 must be authoritative for the designated zone.

The node availability criteria described in section 2.4.1 in this document also apply to this test.

34.6 Special procedural requirements

This test has no procedural requirements.

34.7 Intercase dependencies

This test has no intercase dependencies.

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

A SOA query over UDP and TCP for the designated zone is made for each name server in the input data described in section 19.3. If there are no answers, this test case fails (based on the outcome criteria in 34.4).

[23] https://www.iana.org/help/nameserver-requirements

35. Test Case DNS33: Answer authoritatively (Distributed)

35.1 Test case identifier

DNS33

35.2 Objective

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.

This test case fulfills the requirements 2.4.1 and 2.4.2 in the "Technical requirements for authoritative name servers"[24] document.

35.3 Inputs

See section 19.3 in this document.

35.4 Outcome(s)

After the measurement criteria in section 2.4.1 has been passed, the following outcome must be true for all DNS answers, or this test case fails:

All name servers give authoritative answers over UDP and TCP. If any of the listed name servers in section 19.3 does not answer authoritatively, this test case fail.

35.5 Environmental needs

All authoritative name servers listed in the inputs section 19.3 should be authoritative for the designated zone.

The node availability criteria described in section 2.4.1 in this document also apply to this test.

35.6 Special procedural requirements

This test has no procedural requirements.

35.7 Intercase dependencies

This test has no intercase dependencies.

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

A SOA query over UDP and TCP for the designated zone is made for each name server in the input data described in section 19.3. If any of the name servers fail to give an authoritative answer ("AA-bit" is set in the answer), the test case fails.

[24] https://www.iana.org/help/nameserver-requirements

36. Test Case DNS34: Consistency between delegation and zone (Distributed)

36.1 Test case identifier

DNS34

36.2 Objective

The set of NS records served by the authoritative name servers must match those proposed for the delegation in the parent zone.

This test case fulfills the requirements 2.7.1 in the "Technical requirements for authoritative name servers"[25] document.

36.3 Inputs

See section 19.3 in this document.

36.4 Outcome(s)

After the measurement criteria in section 2.4.1 has been passed, the following outcome must be true for all DNS answers, or this test case fails:

If any extraneous name server is present in the parent data or in the delegated child zone, this test case fails.

36.5 Environmental needs

All authoritative name servers listed in the inputs section 19.3 should be authoritative for the designated zone.

The node availability criteria described in section 2.4.1 in this document also apply to this test.

36.6 Special procedural requirements

This test has no procedural requirements.

36.7 Intercase dependencies

This test has no intercase dependencies.

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

The name server data on the input parameters side is compared to the content of the answers for all the name servers. If there is an inconsistency between the NS record sets, this test fails.

[25] https://www.iana.org/help/nameserver-requirements

37. Test Case DNS35: Name server must be able to provide referral to known subdomains (Distributed)

37.1 Test case identifier

DNS35

37.2 Objective

All name servers must provide a referral with NS, DS and optional glue for the delegated subdomain.

37.3 Inputs

See section 19.3 in this document.

37.4 Outcome(s)

After the measurement criteria in section 2.4.1 has been passed, the following outcome must be true for all DNS answers, or this test case fails:

If the result of the query does not contain NS and DS records in the authority section, this test fails.

37.5 Environmental needs

All authoritative name servers listed in the inputs section 19.3 should be authoritative for the designated zone.

The node availability criteria described in section 2.4.1 in this document also apply to this test.

37.6 Special procedural requirements

This test has no procedural requirements.

37.7 Intercase dependencies

This test has no intercase dependencies.

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

A SOA query for SubDomain from the input parameters is made to all the name servers. The result must contain a DS and NS set for the next link in the delegation chain.

38. Test Case DNS36: RRSIG(SOA) must validate with supplied DS record (DNSSEC)

38.1 Test case identifier

DNS36

38.2 Objective

Confirm that any of the supplied DS records are actually used, directly as ZSK or indirectly as KSK, for signing the zones' SOA record.

38.3 Inputs

See section 17.3 for all input parameters.

38.4 Outcome(s)

If none of the signatures over the SOA-record validate when using the supplied DS-record as a trust anchor, this test case fails.

38.5 Environmental needs

All authoritative name servers listed in the inputs section 17.3 should be authoritative for the designated zone.

38.6 Special procedural requirements

This test has no special procedural requirements.

38.7 Intercase dependencies

This test has no intercase dependencies.

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

1. Load all supplied DS records into a DNSSEC-validating resolver.
2. Retrieve the SOA RR set from the child zone.
3. Retrieve the RRSIG of the SOA RR set from the child zone.
4. Retrieve the DNSKEY RR set from the child zone.
5. Retrieve the RRSIG of the DNSKEY RR set from the child zone.
6. Do a cryptographic validation of the SOA record using the DS records or DS record as trust anchor.
7. The TC ends with pass if it is possible to validate the SOA record using at least one DS record as trust anchor.

39. General

39.1 Glossary

The glossary is available in the Master Test Plan.

39.2 Document change procedures

Document change procedures are documented in the Master Test Plan.