Pre-Delegation Testing

DNS DNSSEC Test Cases

Version C

File name: PDT_DNS_TC_DNSSEC.docx
Last saved: 2013-05-03

Document control

Document information and security

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

Security class	File name
External	PDT_DNS_TC_DNSSEC.docx

Revisions

Date	Version	Name	Description
2013-01-24	PA1	Patrik Wallström	Initial document
2013-01-24	PA2	Rickard Bellgrim	Update text after review
2013-02-06	PA3	Rickard Bellgrim	Add Document Hierarchy and final chapter
2013-02-08	PA4	Patrik Wallström	Anycast updates
2013-02-25	PA5	Patrik Wallström	Updated input parameters
2013-04-04	PA6	Patrik Wallström	Added new test cases from updated SOW
2013-04-08	PA7	Patrik Wallström	Clarified DNSKEY algorithm statement
2013-04-08	B	Staffan Hagnell	Delivery D2 for production
2013-05-03	C	Mats Dufberg	Released

LIST OF CONTENTS

1. Introduction

1.1 Scope

The Pre-Delegation Testing Provider will test the DNS service for the designated zone and verify the resulting answers. The test case described in this document is done using a program for testing the DS records supplied against the DNSKEY records for all the supplied name servers for the designated zone.

1.2 References

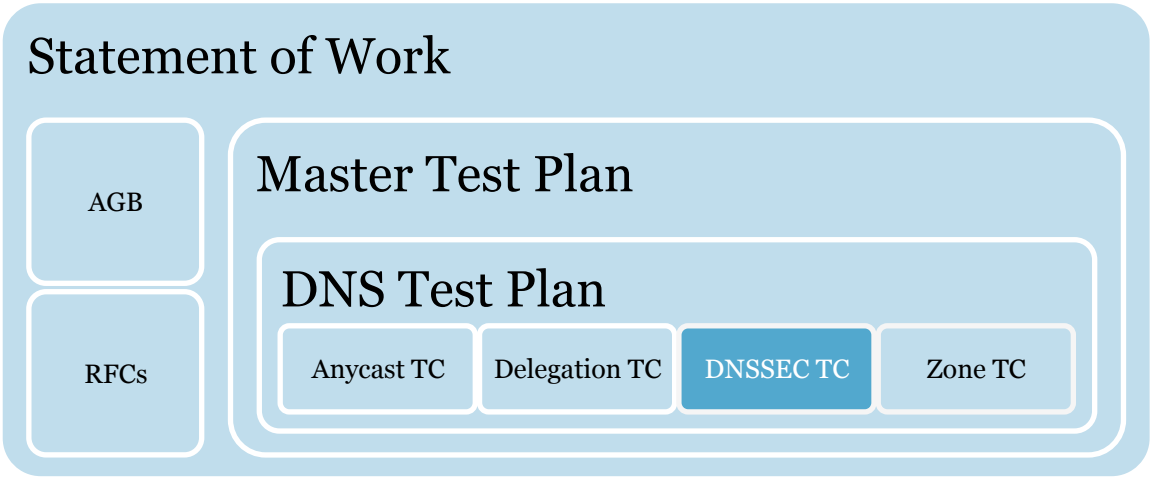
1.2.1 External

- IEEE 829-2008
- ICANN gTLD Applicant Guidebook, Version 2012-06-04
- Placing TLD delegation signer information in the root zone[1]

1.2.2 Internal

- Pre-Delegation Testing, Statement of Work
- Pre-Delegation Testing, Master Test Plan
- Pre-Delegation Testing, DNS Test Plan

1.2.3 Document Hierarchy



1.3 Context

All tests are to be performed over IPv4 and IPv6 from at least five points on the Internet. At least one probe node should be located in every ICANN region.

1.4 Notation for description

Each test case for the DNS service is described in their own section. The test procedures are described directly in the test case.

[1] http://www.iana.org/procedures/root-dnssec-records.html

2. Legal values for the DS hash digest algorithm

2.1 Test case identifier

DNS14 Legal values for the DS hash digest algorithm

2.2 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 "Placing TLD delegation signer information in the root zone" document.

2.3 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
DnsAnycastNameServer-[1..n]	FQDN or IPv4 or IPv6 address for the name server, with optional port numbers	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. In addition to this we need all anycast and unicast name servers and their IPv4 and IPv6 addresses, in addition to the name servers used for publication in the IANA zone. In case of using anycast for any name servers, all unicast addresses for all nodes in the anycast system must be included for testing DNSSEC support.

If the unicast addresses cannot be provided, the applicant must provide a DNS proxy address with port numbers for all the unicast servers in the anycast network.

2.4 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.)

2.5 Environmental needs

This test has no environmental needs.

2.6 Special procedural requirements

This test has no special procedural requirements.

2.7 Intercase dependencies

This test has no intercase dependencies.

2.8 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 2.3. The DnsKeyDigestType input number is compared with the values 1 and 2, where it must match either.

3. DS must match a DNSKEY in the designated zone

3.1 Test case identifier

DNS15 DS must match a DNSKEY in the designated zone

3.2 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 "Placing TLD delegation signer information in the root zone" document.

3.3 Inputs

See section 2.3 for all input parameters.

3.4 Outcome(s)

All submitted DS records must match a DNSKEY that is published on all the name servers (including all unicast nodes in an anycast system) for the designated zone.

80% of the unicast nodes in an anycast network must reply with authoritative answers for this test to pass.

3.5 Environmental needs

All authoritative name servers listed in the inputs section 2.3 should be authoritative for the designated zone.

3.6 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.

3.7 Intercase dependencies

This test has no intercase dependencies.

3.8 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 2.3.

For each DS record from the input parameters, a query for DNSKEY is sent to all specified name servers. There must be a matching DNSKEY in the answer section for all queries made.

4. Signatures in the designated zone must validate

4.1 Test case identifier

DNS16 Signatures in the designated zone must validate

4.2 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.

4.3 Inputs

See section 2.3 for all input parameters.

4.4 Outcome(s)

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.

80% of the unicast nodes in an anycast network must reply with authoritative answers for this test to pass.

4.5 Environmental needs

All authoritative name servers listed in the inputs section 2.3 should be authoritative for the designated zone.

4.6 Special procedural requirements

This test has no special procedural requirements.

4.7 Intercase dependencies

This test has no intercase dependencies.

4.8 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 2.3.

For each name server, a query is sent to all the name servers for the SOA record. The answers must contain a SOA record and an RRSIG record. To follow the chain from the DS to the RRSIG the DNSKEY set found in the previous test case in section 3 is reused (per name server queried).

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

5. Zone contains NSEC or NSEC3 records

5.1 Test case identifier

DNS17 Zone contains NSEC or NSEC3 records

5.2 Objective

Verify that there are NSEC or NSEC3 records present in the zones with valid signatures.

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

5.3 Inputs

See section 2.3 for all input parameters.

5.4 Outcome(s)

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, or if the show an invalid RRSIG, this test fails.

80% of the unicast nodes in an anycast network must reply with authoritative answers for this test to pass.

5.5 Environmental needs

All authoritative name servers listed in the inputs section 2.3 should be authoritative for the designated zone.

5.6 Special procedural requirements

This test has no special procedural requirements.

5.7 Intercase dependencies

This test has no intercase dependencies.

5.8 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 2.3.

A query is made for xx—example.[TLD], a label that should never occur because of the prefix. The answer should contain NSEC or NSEC3 records with valid signatures.

6. Check for too many NSEC3 iterations

6.1 Test case identifier

DNS25 NSEC3 Iterations

6.2 Objective

The number of NSEC3 Iterations must not be too many (150 or more).

This test case is an addition to the Statement of Work; see section 2.1.2 in the DNS Test Plan document.

6.3 Inputs

See section 2.3 in this document.

6.4 Outcome(s)

If the NSEC3 Iterations value is equal to or greater than 150 this test emits a warning.

80% of the unicast nodes in an anycast network must reply with authoritative answers for this test to pass.

6.5 Environmental needs

This test has no environmental requirements.

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

The test program is executed with all of the input parameters described in section 2.3.

The Iterations value from the NSEC3PARAM is retrieved from all specified name servers and compared to the value 150.

7. Check for too short or too long RRSIG lifetimes

7.1 Test case identifier

DNS26 RRSIG Lifetimes

7.2 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 in the DNS Test Plan document.

7.3 Inputs

See section 2.3 for all input parameters.

7.4 Outcome(s)

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

80% of the unicast nodes in an anycast network must reply with authoritative answers for this test to pass.

7.5 Environmental needs

All authoritative name servers listed in the inputs section 2.3 should be authoritative for the designated zone.

7.6 Special procedural requirements

This test has no special 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

The test program is executed with all of the input parameters described in section 2.3.

The RRSIG records are retrieved as described in section 4.8. 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.

8. Check for invalid DNSKEY algorithms

8.1 Test case identifier

DNS27 DNSKEY Algorithms

8.2 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 in the DNS Test Plan document.

8.3 Inputs

See section 2.3 for all input parameters.

8.4 Outcome(s)

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

80% of the unicast nodes in an anycast network must reply with authoritative answers for this test to pass.

8.5 Environmental needs

All authoritative name servers listed in the inputs section 2.3 should be authoritative for the designated zone.

8.6 Special procedural requirements

This test has no special 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

The test program is executed with all of the input parameters described in section 2.3.

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.[2]

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

9. Global

9.1 Glossary

The glossary is available in the Master Test Plan.

9.2 Document change procedures

Document change procedures are documented in the Master Test Plan.