

# **Pre-Delegation Testing**

## **Documentation DNS Test Cases**

**Version G**

File name: PDT\_Documentation\_TC\_DNS.docx  
Last saved: 2013-07-25

Copyright © 2013 Internet Corporation For Assigned Names and Numbers. All rights reserved.

# Document control

## Document information and security

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

Security class	File name
External	PDT_Documentation_TC_DNS.docx

## Revisions

Date	Version	Name	Description
2013-02-01	PA1	Björn Sjöholm	Initial document
2013-02-07	PA2	Björn Sjöholm	Test case 23 moved to DOC SL
2013-02-07	PA3	Rickard Bellgrim	Add Document Hierarchy and final chapter
2013-02-11	PA4	Lennart Bonnevier	Review text
2013-03-01	PA5	Rickard Bellgrim	“KSK/ZSK keys” to “cryptographic keys”
2013-03-05	PA6	Björn Sjöholm	References added. Testcases 17 and 22 deleted. A new testcase 21 added.
2013-03-26	PA7	Björn Sjöholm	Testcases 07, 13 and 17 merged into 02. Testcases 08, 14 and 18 merged into 03. Testcases 09, 15 and 19 merged into 04. Testcases 10, 16 and 20 merged into 05. Testcase 11 renumbered to 07. Testcase 12 renumbered to 08. Testcase 21 renumbered to 09. Clarification of testcase 09
2013-04-18	PA8	Lennart Beckman	Testcase 06 withdrawn. Testcase 07-09 renumbered accordingly.
2013-04-19	B	Mats Dufberg	Released.
2013-05-02	PC1	Lennart Beckman	Misprints corrected regarding numbering of Testcases 07-09
2013-05-02	C	Lennart Beckman	Release
2013-05-03	D	Mats Dufberg	Released
2013-06-12	PE1	Lennart Beckman	PASS/FAIL criteria added
2013-06-17	PE2	Lennart Beckman	Test case titles added. References to application removed. DocDNS08 revised.
2013-06-25	E	Lennart Beckman	Released
2013-07-04	PF1	A. Thulin	Modifications proposed by ICANN, and clarification of adequate defense against DDoS attacks.
2013-07-08	F	Mats Dufberg	Released.
2013-07-16	PG1	Mårten Frosth	Modifications proposed by ICANN, corrections of missing data that should have been included in version F.
2013-07-23	PG2	Mårten Frosth	Modification to DocDNS01 to include specific capacity criteria of 10 times the expected load.

Date	Version	Name	Description
2013-07-24	PG3	Mårten Frosth	Modification to DocDNS01, changed specific capacity criteria from 10x to 2x.
2013-07-24	G	Mårten Frosth	Released.

## LIST OF CONTENTS

<b>1. INTRODUCTION.....</b>	<b>6</b>
1.1 SCOPE .....	6
1.2 REFERENCES .....	6
1.2.1 External.....	6
1.2.2 Internal .....	6
1.2.3 Document Hierarchy .....	6
1.3 CONTEXT.....	6
1.4 NOTATION FOR DESCRIPTION .....	6
<b>2. DOCUMENT DNS 01, CAPACITY AND DDOS MITIGATION .....</b>	<b>7</b>
2.1 TEST CASE IDENTIFIER .....	7
2.2 OBJECTIVE .....	7
2.3 INPUTS .....	7
2.4 OUTCOME(S).....	7
2.5 ENVIRONMENTAL NEEDS.....	7
2.6 SPECIAL PROCEDURAL REQUIREMENTS.....	7
2.7 INTERCASE DEPENDENCIES .....	7
2.8 ORDERED DESCRIPTION OF STEPS TO BE TAKEN TO EXECUTE THE TEST CASE.....	7
<b>3. DOCUMENT DNS 02, LOAD CAPACITY, LATENCY AND NETWORK REACHABILITY .....</b>	<b>9</b>
3.1 TEST CASE IDENTIFIER .....	9
3.2 OBJECTIVE .....	9
3.3 INPUTS .....	9
3.4 OUTCOME(S).....	9
3.5 ENVIRONMENTAL NEEDS.....	9
3.6 SPECIAL PROCEDURAL REQUIREMENTS.....	9
3.7 INTERCASE DEPENDENCIES .....	9
3.8 ORDERED DESCRIPTION OF STEPS TO BE TAKEN TO EXECUTE THE TEST CASE.....	9
<b>4. DOCUMENT DNS 03, LOAD CAPACITY TABLES AND GRAPHS .....</b>	<b>11</b>
4.1 TEST CASE IDENTIFIER .....	11
4.2 OBJECTIVE .....	11
4.3 INPUTS .....	11
4.4 OUTCOME(S).....	11
4.5 ENVIRONMENTAL NEEDS.....	11
4.6 SPECIAL PROCEDURAL REQUIREMENTS.....	11
4.7 INTERCASE DEPENDENCIES .....	11
4.8 ORDERED DESCRIPTION OF STEPS TO BE TAKEN TO EXECUTE THE TEST CASE.....	11
<b>5. DOCUMENT DNS 04, 20 DATA POINTS .....</b>	<b>13</b>
5.1 TEST CASE IDENTIFIER .....	13
5.2 OBJECTIVE .....	13
5.3 INPUTS .....	13
5.4 OUTCOME(S).....	13
5.5 ENVIRONMENTAL NEEDS.....	13
5.6 SPECIAL PROCEDURAL REQUIREMENTS.....	13
5.7 INTERCASE DEPENDENCIES .....	13
5.8 ORDERED DESCRIPTION OF STEPS TO BE TAKEN TO EXECUTE THE TEST CASE.....	13
<b>6. DOCUMENT DNS 05, QUERY LATENCY .....</b>	<b>15</b>
6.1 TEST CASE IDENTIFIER .....	15
6.2 OBJECTIVE .....	15
6.3 INPUTS .....	15
6.4 OUTCOME(S).....	15
6.5 ENVIRONMENTAL NEEDS.....	15
6.6 SPECIAL PROCEDURAL REQUIREMENTS.....	15
6.7 INTERCASE DEPENDENCIES .....	15
6.8 ORDERED DESCRIPTION OF STEPS TO BE TAKEN TO EXECUTE THE TEST CASE.....	15

<b>7.</b>	<b>DOCUMENT DNS o6, TCP REACHABILITY .....</b>	<b>17</b>
7.1	TEST CASE IDENTIFIER .....	17
7.2	OBJECTIVE .....	17
7.3	INPUTS .....	17
7.4	OUTCOME(S) .....	17
7.5	ENVIRONMENTAL NEEDS .....	17
7.6	SPECIAL PROCEDURAL REQUIREMENTS .....	17
7.7	INTERCASE DEPENDENCIES .....	17
7.8	ORDERED DESCRIPTION OF STEPS TO BE TAKEN TO EXECUTE THE TEST CASE .....	17
<b>8.</b>	<b>DOCUMENT DNS o7, BASIC DNSSEC SUPPORT .....</b>	<b>19</b>
8.1	TEST CASE IDENTIFIER .....	19
8.2	OBJECTIVE .....	19
8.3	INPUTS .....	19
8.4	OUTCOME(S) .....	19
8.5	ENVIRONMENTAL NEEDS .....	19
8.6	SPECIAL PROCEDURAL REQUIREMENTS .....	19
8.7	INTERCASE DEPENDENCIES .....	19
8.8	ORDERED DESCRIPTION OF STEPS TO BE TAKEN TO EXECUTE THE TEST CASE .....	19
<b>9.</b>	<b>DOCUMENT DNS o8, NAMESERVER CONSISTENCY .....</b>	<b>21</b>
9.1	TEST CASE IDENTIFIER .....	21
9.2	OBJECTIVE .....	21
9.3	INPUTS .....	21
9.4	OUTCOME(S) .....	21
9.5	ENVIRONMENTAL NEEDS .....	21
9.6	SPECIAL PROCEDURAL REQUIREMENTS .....	21
9.7	INTERCASE DEPENDENCIES .....	21
9.8	ORDERED DESCRIPTION OF STEPS TO BE TAKEN TO EXECUTE THE TEST CASE .....	21
<b>10.</b>	<b>GLOBAL .....</b>	<b>23</b>
10.1	GLOSSARY .....	23
10.2	DOCUMENT CHANGE PROCEDURES .....	23

## 1. Introduction

---

### 1.1 Scope

The Pre-Delegation Testing Provider will test self-certification documents regarding DNS and verify that the requirements are fulfilled.

### 1.2 References

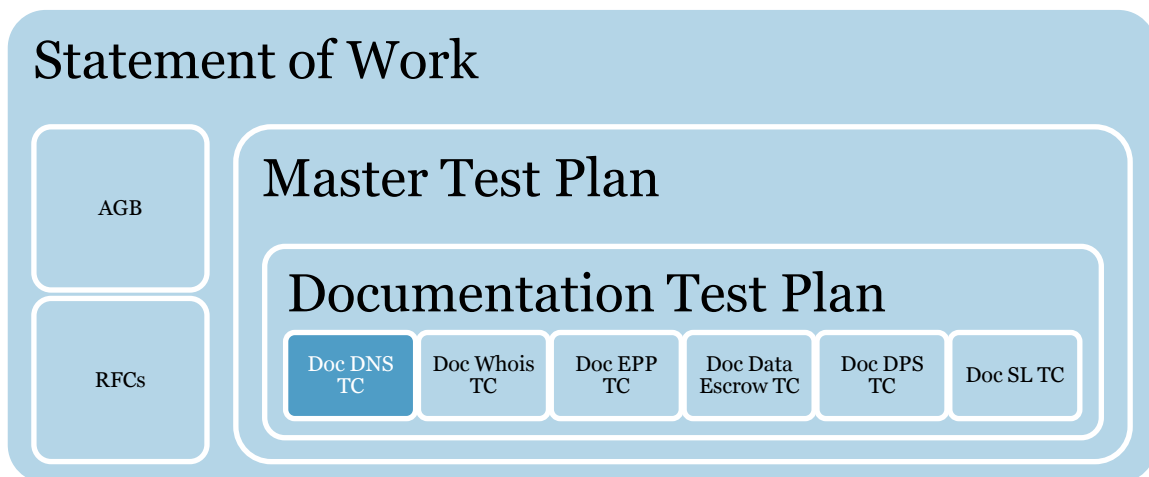
#### 1.2.1 External

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

#### 1.2.2 Internal

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

#### 1.2.3 Document Hierarchy



### 1.3 Context

N/A

### 1.4 Notation for description

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

## 2. Document DNS 01, Capacity and DDOS Mitigation

---

### 2.1 Test case identifier

DocDNS01 Capacity and DDOS Mitigation

### 2.2 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.

### 2.3 Inputs

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

Id	Description	Type
gTLDSelfCert	The Applicants self-certification documentation	Documents

### 2.4 Outcome(s)

The self-certification documents **MUST** include the required information.

### 2.5 Environmental needs

N/A

### 2.6 Special procedural requirements

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

### 2.7 Intercase dependencies

This test has no intercase dependencies.

### 2.8 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.



### 3. Document DNS 02, Load Capacity, Latency and Network Reachability

---

#### 3.1 Test case identifier

DocDNS02 Load Capacity, Latency and Network Reachability

#### 3.2 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.

#### 3.3 Inputs

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

Id	Description	Type
gTLDSelfCert	The Applicants self-certification documentation	Documents

#### 3.4 Outcome(s)

The self-certification documents **MUST** include the required information.

#### 3.5 Environmental needs

N/A

#### 3.6 Special procedural requirements

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

#### 3.7 Intercase dependencies

This test has no intercase dependencies.

#### 3.8 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.

## 4. Document DNS 03, Load Capacity Tables and Graphs

---

### 4.1 Test case identifier

DocDNS03 Load Capacity Tables and Graphs

### 4.2 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.

### 4.3 Inputs

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

Id	Description	Type
gTLDSelfCert	The Applicants self-certification documentation	Documents

### 4.4 Outcome(s)

The self-certification documents **MUST** include the required information.

### 4.5 Environmental needs

N/A

### 4.6 Special procedural requirements

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

### 4.7 Intercase dependencies

This test has no intercase dependencies.

### 4.8 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.

## 5. Document DNS 04, 20 Data Points

---

### 5.1 Test case identifier

DocDNS04 20 Data Points

### 5.2 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 applicant's DNS infrastructure.

The test also verifies that the query response include either contains zone data or are NXDOMAIN or NODATA responses.

### 5.3 Inputs

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

Id	Description	Type
gTLDSelfCert	The Applicants 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 applicant 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 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 applicant's DNS infrastructure.
3. Verify that the responses are shown to
  - a. either contain zone data or
  - b. be NXDOMAIN or NODATA responses.

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).
- Responses are stated to be either contain zone data or are NXDOMAIN or NODATA (step 3).

Criteria for FAIL:

- Part of the requested information is unclear or missing.

## 6. Document DNS 05, Query Latency

---

### 6.1 Test case identifier

DocDNS05 Query Latency

### 6.2 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.

### 6.3 Inputs

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

Id	Description	Type
gTLDSelfCert	The Applicants 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 applicant 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 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.



## 7. Document DNS 06, TCP Reachability

---

### 7.1 Test case identifier

DocDNS06 TCP Reachability

### 7.2 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.

### 7.3 Inputs

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

Id	Description	Type
gTLDSelfCert	The Applicants 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 applicant 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 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.

## 8. Document DNS 07, Basic DNSSEC Support

---

### 8.1 Test case identifier

DocDNS07 Basic DNSSEC Support

### 8.2 Objective

The test verifies that the self-certification documents for DNSSEC support 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.

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

### 8.3 Inputs

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

Id	Description	Type
gTLDSelfCert	The Applicants 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 applicant 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 cover DNSSEC support. Expected part is: document gTLDSelfCert section 1.4.
2. Verify that it demonstrates
  - 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 demonstrates 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).

Criteria for FAIL:

- Part of the requested information is unclear or missing.

## 9. Document DNS 08, Nameserver Consistency

---

### 9.1 Test case identifier

DocDNS08 Nameserver Consistency

### 9.2 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.

### 9.3 Inputs

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

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

### 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 applicant 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 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.

## 10. Global

---

### 10.1 Glossary

The glossary is available in the Master Test Plan.

### 10.2 Document change procedures

Document change procedures are documented in the Master Test Plan.