RST Documentation Self-certification

Submitted to ICANN by: <Registry Operator>

String (A-label): <TLD>

Template Version: 2.1.0, Date: 2017-07-27

Registry Operator's Revision Date: <day month year>

About this document

This document provides a template and instructions for the self-certification documentation for the Registry System Testing ("RST"). The document is provided in different formats, including pdf.

The self-certification document created by the Registry Operator shall follow the structure, headings and numbering given in this document, and must be submitted in pdf-format.

The document shall consist of the Registry Operator´s statements and certification that the requirements are fulfilled. Unless otherwise stated, the basis for the information can, in many cases, be decided by the Registry Operator. As an example, information may be derived by performing actual tests, by using statistical data or by deduction from similar systems.

The self-certification documentation shall comply with
- the requirements stated in Module 5 of the gTLD Applicant Guidebook, AGB.
- the requirements stated in the Registry Agreement including, but not limited to, Exhibit A and the specifications 2,4,6 and 10.

The Registry Operator shall provide the information described below. The template is based on the requirements in the AGB.

1. DNS infrastructure

> AGB, chapter 5.2.2:
> All tests shall be done both over IPv4 and IPv6, with reports providing results according to both protocols.

> AGB, chapter 5.2.2:
> Self-certification documentation shall include data on load capacity, latency and network reachability.

1.1. Load capacity

1.1.1. Expected load

Instruction: Describe the expected load on the name servers during normal operation, for both IPv4 and IPv6. If servers serve additional zones, then the load of these other zones must be taken into consideration.

Give a short justification of the figures. If a shared name server is used, describe it briefly.

Registry Operator self-certification:

1.1.2. Statistical population

> AGB, chapter 5.2.2:
> The load capacity test shall be performed against a randomly selected subset of servers within the [Registry Operator's] DNS infrastructure.

Instruction: Describe briefly the selected subset, how it has been selected and what percentage of the total set of servers it represents. This applies to both IPv4 and IPv6.

Registry Operator self-certification:

1.1.3. Method

> AGB, chapter 5.2.2:
> Responses must either contain zone data or be NXDOMAIN or NODATA responses to be considered valid.

> AGB Module 5, Registry Agreement, specification 10, section 3.11:
> Placement of DNS probes. Probes for measuring DNS parameters shall be placed as near as possible to the DNS resolvers on the networks with the most users across the different geographic regions; care shall be taken not to deploy probes behind high propagation-delay links, such as satellite links.

Instruction: Describe the method of measurement. Document the types of responses received (zone data, NXDOMAIN, NODATA, etc.)

Registry Operator self-certification:

1.1.4 Detecting and Mitigating DDoS attacks

Instruction: Describe your strategy for detecting and mitigating Distributed Denial of Service (DDoS) attacks. Also describe the controls you use.

Registry Operator self-certification:

1.1.5. Result

> AGB, chapter 5.2.2:
> Load capacity shall be reported using a table and a corresponding graph, showing percentage of queries responded against an increasing number of queries per second generated from local (to the servers) traffic generators. The table shall include at least 20 data points and loads of UDP-based [and TCP-based] queries that will cause up to 10% query loss against a randomly selected subset of servers within the [Registry Operator's] DNS infrastructure.

> AGB, chapter 5.2.2:
> Load capacity [...] [for DNSSEC support] shall be documented as for UDP and TCP above.

> AGB, chapter 5.2.2:
> The documentation provided by the [Registry Operator] must include the results from a system performance test indicating available network and server capacity and an estimate of expected capacity during normal operation to ensure stable service as well as to adequately address Distributed Denial of Service (DDoS) attacks.

Instruction*:*

- Provide names, geographical locations and IPv4/IPv6 addresses of all authoritative nameservers (unicast and anycast).
- Describe briefly your nameserver setup (unicast and/or anycast).
- If using anycast, describe briefly your anycast solution.
- Document briefly results from system performance test showing available network and server capacity.
- Describe an estimate of expected capacity during normal operation.
- Create one table and graph for IP4 and one for IPv6 according to the requirements below.
    - The table shall include at least 20 data points.

- The table shall include loads that cause up to 10% query loss against a randomly selected subset of servers, or a maximum of 100000 queries per second.
- The table shall cover both UDP and TCP.
- The table shall cover DNSSEC for both UDP and TCP.

Examples can be found below.

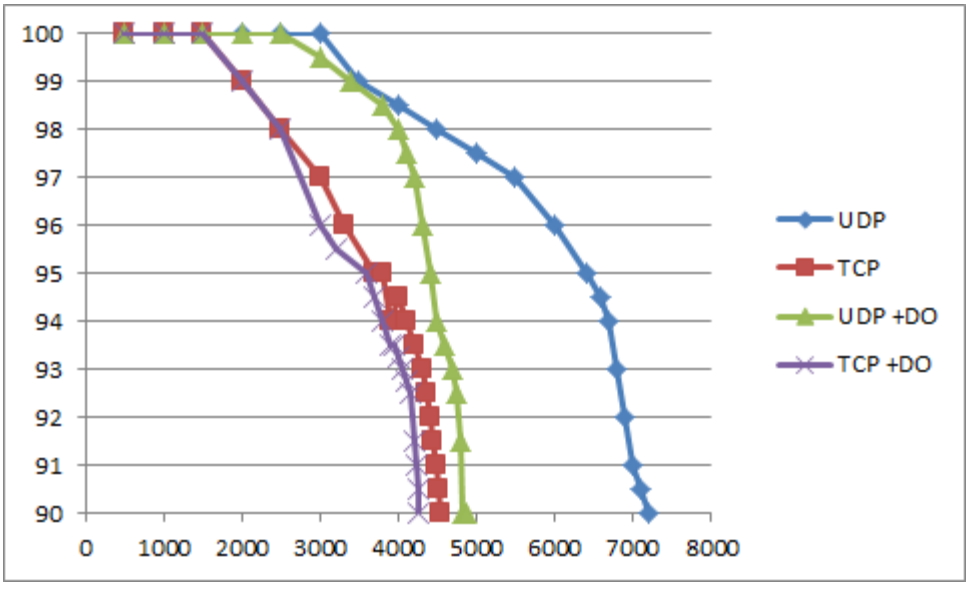
Registry Operator self-certification:

Example table showing percentage of queries responded against an increasing number of queries per second:

	UDP		TCP		UDP +DO		TCP +DO	
#	QPS	%	QPS	%	QPS	%	QPS	%
1	500	100	500	100	500	100	500	100
2	1000	100	1000	100	1000	100	1000	100
3	1500	100	1500	100	1500	100	1500	100
4	2000	100	2000	99	2000	100	2000	99
5	2500	100	2500	98	2500	100	2500	98
6	3000	100	3000	97	3000	99.5	3000	96
7	3500	99	3300	96	3400	99	3200	95.5
8	4000	98.5	3700	95	3800	98.5	3600	95
9	4500	98	3800	95	4000	98	3700	94.5

10	5000	97.5	3900	94	4100	97.5	3800	94
11	5500	97	4000	94.5	4200	97	3900	93.5
12	6000	96	4100	94	4300	96	3950	93.5
13	6400	95	4200	93.5	4400	95	4000	93.25
14	6600	94.5	4300	93	4500	94	4050	93
15	6700	94	4350	92.5	4600	93.5	4100	92.75
16	6800	93	4400	92	4700	93	4150	92.5
17	6900	92	4450	91.5	4750	92.5	4200	91.5
18	7000	91	4500	91	4800	91.5	4225	91
19	7100	90.5	4525	90.5	4825	90	4250	90.5
20	7200	90	4550	90	4875	90	4260	90

Example graph:



1.2. Query latency

> AGB, chapter 5.2.2:
> Query latency shall be reported in milliseconds as measured by DNS probes located just outside the border routers of the

> physical network hosting the name servers, from a network topology point of view.

1.2.1. Method

Instruction: Describe briefly how the query latency has been measured.

Registry Operator self-certification:

1.2.2. Result

Instruction: Report the min/avg/max values of query latency in milliseconds. The test shall include both UDP and TCP. The tests shall also include DNSSEC. Perform and report the tests for all name servers (IPv4/IPv6).

Registry Operator self-certification:

Example table showing query latency (min/avg/max) in milliseconds:

NS	IP	UDP	TCP	UDP +DO	TCP +DO

a.ns.TLD	192.0.2.1	120/125/134	150/151/152	122/140/200	152/160/171
a.ns.TLD	2001:DB8::1	100/103/109	125/126/127	110/115/116	135/141/145
b.ns.TLD	192.0.2.2	90/91/92	90/93/94	91/91/92	91/97/100
b.ns.TLD	2001:DB8::2	98/99/103	110/115/118	105/125/190	107/130/200
c.ns.TLD	192.0.2.3	50/55/60	53/54/55	60/69/81	70/71/72

1.3. Reachability

1.3.1. Reachability TCP-based DNS queries

> AGB, chapter 5.2.2:
> Reachability will be documented by providing records of TCP-based DNS queries from nodes external to the network hosting the servers. These locations may be the same as those used for measuring latency for TCP support above.

Instruction: Provide the information specified by the requirement above. One TCP-based DNS query record for each name server is sufficient. Repeat for both IPv4 and IPv6.

Registry Operator self-certification:

1.3.2. Network Reachability

Instruction: Document network reachability information by providing information on the transit and peering arrangements for the DNS server locations, listing the AS numbers of the transit providers or peers at each point of presence and available bandwidth at those points of presence.

Registry Operator self-certification:

1.4 DNSSEC

```
AGB, chapter 5.2.2:
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.
```

Instruction:
Provide information that demonstrates

- support for EDNS(0) in the server infrastructure.
- the ability to return correct DNSSEC-related resource records (e.g. DNSKEY, RRSIG, NSEC/NSEC3) for the signed zone.
- the ability to accept and publish DS resource records from second-level domain administrators.
- the Registry Operators ability to support the full life cycle of cryptographic keys.

Registry Operator self-certification:

1.5. SLA, DNS Infrastructure

Instruction:
Provide a table describing the adherence to the SLA Service Level Requirements as given in Specification 10 of the Registry Agreement.

Registry Operator self-certification:

Template table showing adherence to the SLA:

Parameter	**Self-certification (monthly basis)**
DNS service availability	____ min downtime
DNS name server availability	≤ ____ min of downtime
TCP DNS resolution RTT	≤ ____ ms, for at least 95% of the queries
UDP DNS resolution RTT	≤ ____ ms, for at least 95% of the queries
DNS update time	≤ ____ min, for at least 95% of the probes

2. Whois

> AGB, chapter 5.2.3:
> [Registry Operator] must provide Whois services for the anticipated load. ICANN will verify that Whois data is accessible over IPv4 and IPv6 via both TCP port 43 and via a web interface and review self-certification documentation regarding Whois transaction capacity.

2.1. Load capacity

> AGB, chapter 5.2.3:
> Self-certification documents shall describe the maximum number of queries per second successfully handled by both the port 43 servers as well as the web interface, together with an [Registry Operator]-provided load expectation.

2.1.1. Expected load

Instruction: Describe the expected load on the Whois service (port 43 and HTTP) during normal operation. If it is a Shared Registry System, then the load of other TLD:s must be taken into consideration. Do this for IPv4 only.

Describe the shared registry system, if applicable.

Registry Operator self-certification:

2.1.2. Port 43

2.1.2.1. Method

Instruction: Describe briefly how the load capacity has been measured.

Registry Operator self-certification:

2.1.2.2. Result

Instruction: Describe the maximum number of queries per second successfully handled by the port 43 servers.

Registry Operator self-certification:

2.1.3. HTTP

2.1.3.1. Method

Instruction: Describe briefly how the load capacity has been measured.

Registry Operator self-certification:

2.1.3.2. Result

Instruction: Describe the maximum number of queries per second successfully handled by the web interface.

Registry Operator self-certification:

2.2. Data mining

```
AGB, chapter 5.2.3:
Additionally, a description of deployed control functions to
detect and mitigate data mining of the Whois database shall
be documented.
```

Instruction: Describe the control functions for detection and mitigation of data mining of the Whois database.

The description should cover both the strategy used and implemented controls.

Registry Operator self-certification:

2.3. SLA, Whois

AGB, chapter 5.2.3:
System performance -- The registry system must scale to meet the performance requirements described in specification 10 of the registry agreement.

Instruction:
Provide a table describing the adherence to the SLA Service Level Requirements as given in Specification 10 of the Registry Agreement.

Registry Operator self-certification:

Template table showing adherence to the SLA:

Parameter	**Self-certification (monthly basis)**
RDDS availability	____ min downtime
RDDS query RTT	≤ ____ ms, for at least 95% of the queries
RDDS update time	≤ ____ min, for at least 95% of the probes

3. EPP

3.1. Load capacity

Instruction:

- Provide the anticipated normal load on the EPP service.
- Provide the EPP service load capacity.
- Describe briefly the expected registry database size (nr of domains) after one year of operation.
- Provide the expected transaction per second rate as a function of the registry database size. The description shall contain at least 10 data points ranging from an empty database to the expected size after one year.

Registry Operator self-certification:

Example table showing the load capacity:

#	Number of domains	Expected TPS
1	0	2000
2	200000	1900
3	250000	1850
4	300000	1825
5	350000	1800
6	400000	1775
7	500000	1750

8	650000	1700
9	800000	1625
10	1000000	1550

3.2. Initial load

> AGB, chapter 5.2.3:
> Documentation shall also describe measures taken to handle load during initial registry operations, such as a land-rush period.

Instruction: Describe briefly how the load is handled for the initial registry operations, such as a land-rush period. A justification of the chosen solution should be provided.

Registry Operator self-certification:

3.3. EPP Extensions

Instruction:

- Describe briefly how all provided EPP extensions are documented in accordance with RFC 3735.

Registry Operator self-certification:

3.4. SLA, EPP

AGB, chapter 5.2.3:
System performance -- The registry system must scale to meet the performance requirements described in specification 10 of the registry agreement.

Instruction:
Provide a table describing the adherence to the SLA Service Level Requirements as given in Specification 10 of the Registry Agreement.

Registry Operator self-certification:

Example table showing adherence to the SLA:

Parameter	**Self-certification (monthly basis)**
EPP service availability	____ min downtime
EPP session-command RTT	≤ ____ ms, for at least 90% of the commands
EPP query-command RTT	≤ ____ ms, for at least 90% of the commands
EPP transform-command RTT	≤ ____ ms, for at least 90% of the commands

4. Escrow Agreement

The Data Escrow Agreement forms part of the Registry Agreement stated in Module 5 of the AGB.

> AGB, chapter 5.1, Registry Agreement:
> The Registry Agreement can be reviewed in the attachment to this module.
> ... All successful [Registry Operators] are expected to enter into the agreement substantially as written.

> AGB, chapter 5.2.1, Testing Procedures:
> The [Registry Operator] [shall submit] all of the following information:
> ... The executed agreement between the selected escrow agent and the [Registry Operator].

> Registry Agreement, Specification 2,
> Data Escrow Requirements:
>
> Registry Operator will engage an independent entity to act as data escrow agent ("Escrow Agent") for the provision of data escrow services related to the Registry Agreement. The following Technical Specifications set forth in Part A, and Legal Requirements set forth in Part B, will be included in any data escrow agreement between Registry Operator and the Escrow Agent, under which ICANN must be named a third-party beneficiary. In addition to the following requirements, the data escrow agreement may contain other provisions that are not contradictory or intended to subvert the required terms provided below.

Specification:
The Registry Operator must provide an executed escrow agreement (signed by the Registry Operator and the approved data escrow agent) substantially as written in specification 2 to the Registry Agreement as stated in AGB Module 5. ICANN approved data escrow agents are listed in https://newgtlds.icann.org/en/applicants/data-escrow.

In addition the Registry Operator must provide written approval of the executed escrow agreement either by

i) a duly executed letter of compliance (signed by the data escrow agent) serving as self certification that all requirements in Specification 2, including both the Technical Specifications set forth in Part A and Legal Requirements set forth in Part B are met, or

ii) a duly executed letter of compliance from ICANN for non standard escrow agreements.

The effective date of the escrow agreement and the date on letter of compliance must be a date prior to submitting the documents for RST testing.

Registry Operator checklist:

[ ] Executed escrow agreement has been uploaded.

[ ] Written approval from escrow agent or ICANN, as relevant, has been uploaded.

5. IDN

The IDN section has been moved to the IDN Self-certification template.

6. Searchable Whois

Instruction:
Do you intend to support searchability capabilities on the Directory-Services and if so do you comply with the specifications described in Specification 4 of the Registry Agreement?

[ ] Yes

[ ] No