The DENIC Comments to *Technical Checks Used for DNS Root Zone Changes*

September 29th, 2006

1 Introduction

This is DENIC's detailed response to ICANN's request for comments on the so called *Technical Checks Used for DNS Root Zone Changes*. We will follow the structure of the paper by first addressing the checks numbered 1 through 11, then responding to the guiding questions and, after commenting on tests 12 through 16, making some general remarks.
DENIC, as the ccTLD Manager for .de, appreciates the current procedure being made subject to public review and comment. This gives opportunity for clarification, refinement and overall improvement of the root zone change process.

1.1 Guiding Principles

While DENIC fully supports IANA's goals to ensure stability and security with regard to the management of the DNS root, it is also important to recognize that the assurance of the stability and the security of a ccTLDs is the responsibility of the respective ccTLD manager, who is accountable to the respective local Internet community. That said, it is very important to have a clear understanding of each and every check's reason and purpose to avoid unnecessary or inappropriate interference.
With regard to the IANA function, technical checks should therefore only be implemented either to avoid misconfiguration or malfunction of the global root server system or to prevent adverse effects on third parties.

Additional features like the measurement of TLD performance, technical quality scoring, consumer protection etc. are, for good reasons, not part of the IANA function. These issues should and, by the way, are dealt with in other areas. Multiple providers exist, who – either under contract to the TLD operator or on their own behalf – perform quality measurement with results made available to the public.

2 Test Review

We would first like to address in detail the tests listed as currently being applied. For easier understanding, the test descriptions are included in italics.

2.1 IANA Test Walkthrough

1. Minimum number of name servers

> *There must be at least two name servers supplied, and they must not share the same IP address.*

DENIC agrees that this is a reasonable requirement, provided the uniqueness of IP addresses is also applied for multihomed hosts. However, this test needs more of a rationale than just a reference to RFC 1034 and 1035 since in the age of anycast the requirement of „at least two nameservers“ could be achieved by other means.

2. Maximum number of name servers

> *There must be no more than 13 name servers supplied.*

Given that this upper limit exists to avoid or limit situations in which referral responses served by the root name servers need to be truncated or otherwise cut below reason, provoking subsequent TCP queries to the root name servers, this test needs to be refined to actually address the packet size and RRSet selection. We would like to point to the internet-draft actively discussed in the IETF DNS OPerations working group that explicitly addresses this issue, as well as RFC 4472. The fine tuning of this test should be discussed based on these documents.

3. Hostname validity

> *The supplied hostnames for the authoritative name servers must be fully qualified domain names, with labels no longer than 63 octets.*

Provided that this requirement is proposed to avoid adverse effects on the Internet DNS infrastructure, we agree that this is a reasonable approach, as soon as it is spelled out in detail with reference to RFCs 952, 1123, 1034, i.e. length requirements for name server names and LDH syntax should be added.

4. Name server reachability

> *The supplied authoritative name servers should be verifiably reachable over the public Internet. IANA sends a DNS query over UDP for the SOA record of the toplevel domain, and looks for a DNS answer in response. IANA sends the query from its American facilities, and should that fail, tests it from sites in Europe and the Asia-Pacific. If IANA is unable to receive DNS answer packets in response to those queries from any location, or if the IP address under test has limited connectivity that appears unreliable, IANA clarifies the situation with the requestor.*

We understand that this is a prerequisite for the following tests (5), (6), and (9), not to have merits on its own. We would like to emphasize that DENIC does regard performance or QoS issues to not be IANA's business. That said, IANA must ensure that any such test actually addresses the reachability of the TLD name servers, not IANA's connectivity. We would like to add that there already are public services monitoring the responses of TLD name servers, such as RIPE NCC's DNSMON.

5. Name server authority

> *In response to a query for the SOA record for the top-level domain, each of the supplied authoritative name servers must respond with a DNS answer with the AA bit set. (see RFC 1035, Section 4.1.1)*

DENIC would accept this test as reasonable provided the specification is enhanced, to include the exact query parameters (including, e.g., packet header bits) and pending those remarks provided in reponse to *guiding question* (3).

6. Name server coherency

> *IANA checks that the requested name servers match the NS Resource Record set in the children. IANA queries the NS RR-set returned by the authoritative name servers, and compare them to the supplied NS records for the root zone. These should match.*

DENIC does not have issues with this requirement.

7. Glue coherency with hostname

> *IANA checks the A and AAAA records of the authoritative name servers, and compares them to the supplied glue records for inclusion in the root zone. These should match.*

DENIC considers this a reasonable check pending general remarks on glue issues. However, the exact way of determining the address records for the NS records' targets needs to be specified to avoid side effects during changes originating from the self referential nature of glue address records.

8. Glue coherency with existing glue

> *IANA checks if other top-level domains use the supplied glue if the request represents an alteration to the name server's IP address. If the name server hostname is shared, it is not a technical failure per se, but IANA advises the applicant that it requires consensus from all affected parties, and starts a dialogue to check whether or not to proceed. (Note: this particular practice is the subject of a separate forthcoming IANA discussion paper)*

DENIC believes that not only is this test useless, given the previous one, but ill advised and actually detrimental to DNS stability. Since a separate proposal is to be expected, we will refrain from exploring the details and look forward to participating in those deliberations. DENIC would like to see review of this test addressed with priority.

9. Serial number coherency

> *IANA checks the serial numbers in the SOA records supplied by the authoritative name servers. These should match*.

Given that many TLD operators apply frequent changes to TLD zones, this test is likely to generate too many false warnings. There might be only very short periods of time where all SOA RRs show the same serial number – or none at all. In addition, with the use of anycast servers, there is no way to judge the correct zone propagation to all authoritative servers anyway. While amendments to this test could be designed, including intervals for serial numbers (taking into account RFC 1982 arithmetic), DENIC believes that the correct update and dissemination of the zone or zone file should be left to the sole discretion of the TLD operator and therefore suggests this test be dropped.

10. Minimum network diversity

> *IANA asks that the name servers be on geographically and network topologically separated networks. IANA currently loosely tests this by querying with the applicant on their network setup should all name servers be in the same /24 IPv4 range.*

While DENIC believes that topological diversity is a reasonable as well as achievable goal, we do not see IANA in the position to address this performance and quality of service issue. Only to the extent that lack of diversity has potential adverse effects on third parties (i.e., being neither related to the querier nor to the TLD operator or a delegated domain holder), should this issue be of concern. We would also like to repeat our references to anycast technology, which might be applied in a way suggesting little diversity while in fact providing it sufficiently and significantly. With reference to *geographically . . . separated networks* DENIC would like to express the concern that there will be no way to execute this test in an efficient, automated and reasonably accurate manner. In addition, exact geographical location of sites and servers might be considered confidential by the TLD operator. We consider this particular issue not subject to IANA's tasks and ask it be dropped.

11. Name server continuity

> *Should the request involve completely changing every NS record in the root, IANA asks the requestor to consider staggering the request in two passes such that any unexpected faults might be mitigated*.

While a change of the complete NS RRSet can be fully reasonable in case of a redelegation, of change of the infrastructure provider, or otherwise, it might also be indicative of a typographic error. Therefore, a warning might be issued but IANA should not insist on splitting the change request.

2.2 Responses to Guiding Questions

1. *Which technical requirements should be mandatory for TLD operators to comply with in order for changes to be accepted in the DNS root?*

Checks should be distinguished as either syntactical or operational checks, where the former can be applied to the provided data while the latter require issuing actual DNS queries to the proposed authoritative servers or elsewhere. Tests (1) through (7) should be mandatory, tests (8) and (9) should be dropped and tests (10) and (11) only have warning level. Failure to pass test (4) and, subsequently, tests (5) or (6), should be dealt with as mentioned below.

2. *Which issues should be highlighted as warnings by the technical review process?*

As mentioned above, tests (10) and (11) should have warning level only. Additional checks for support of EDNS0 (RFC 2671) or AAAA anomalies (RFC 4074) may be applied, provided they have been presented with sufficient detail and have been reviewed and accepted by the community. However, additional checks of this kind should not clutter the change process.

3. *Under which circumstances should these warnings be allowed to advance if the TLD operator wishes to still proceed?*

If issues are at a warning level, there is no justification not to process the request. The more interesting question is, though, under what circumstances a request should be processed in spite of failing mandatory check(s). There are exceptional situations in which recovery from errors can only happen incrementally. In these situations, for the sake of progress and stability, errors should be ignored if the requested change improves the situation (e.g. "repairing" one of two failed servers).
Failure to pass test (4) should lead to manual inspection in the course of which discussion with the TLD operator should be able to override a negative test result.

4. *How should these technical requirements be implemented in an automated environment?*

All tests, mandatory to pass or warning level, must be specified and made public in all possible detail.
The checking code must be publicly available for testing and inspection, to enable every member of the community to verify the implementation's adherence to the specification. Failure to pass one of the mandatory tests should be brought to the attention of the TLD operator and IANA as soon as possible to resolve the issue and to avoid any delay in processing the change request.
For the automated interface DENIC would like to suggest a two-tiered model where the requesting TLD manager can choose, in advance, to either treat warnings as errors or have the request pass even in the presence of warnings.

5. *What role, if any, should IANA play in the ongoing verification of compliance by TLD operators to minimum technical standards?*

IANA has no supervisory role for TLD operators. Therefore, DENIC does not see any basis for ongoing tests.

3 The *Zone Editor*'s Role
Upon reading of the request for comments, we were surprised to read the following statement:

> *VeriSign, in its role as implementor of IANA-approved changes to the primary root name server, additionally tests for the following characteristics which are NOT tested by IANA during its processing:*

It is not obvious from the *high level process flow* diagram shown under <http://www.iana.org/procedures/process-flow.html> that these tests were specified by and executed under VeriSign's control.
In DENIC's opinion the zone editor should not be entitled to any operational, interactive checks on its own. Since the editor's task, according to our understanding, is to deliver a distributable, loadable root zone it should check the outcome of its editorial work for conformance with the relevant standards and BCPs. Those checks must be constrained to only ensure that the zone file itself adheres to the standards, most notably RFCs 952, 1034, 1035, 1123, 2181 and 2308.

Without being exhaustive, such checks might include

- Length and character set of all domain names involved
- Presence and correctness of a single SOA RR
- Increasing serial number (of the root zone's SOA RR)
- TTL homogeneity throughout RRSets
- Uniqueness of RRs

It should be noted that the root zone file is not only distributed to the root name servers but also to the public. The root zone file must be loadable by standards conformant name servers (that would suggest adding an explicit TTL value to the SOA RR in the current root zone, for instance).
The zone editor must not be allowed to add zone content on its own.
The zone editor should preserve the order of RRs, even though the standards do not specify that.

3.1 Additional Tests by the Zone Editor
The following comments assume that these tests, if at all, will be carried out by IANA subject to the same general considerations as tests 1 through 11.

12. *Whether the name servers have matching PTR records (both IPv4 and IPv6)*

While providing for DNS reverse mapping is, without doubt, good practice, DENIC does not see this as a mandatory requirement. A warning or informational note might be issued for missing or inconsistent PTR RRs in the reverse space.

13. *Whether the name servers have RFC 1918 addresses. (Note: supplying such an address would ordinarily fail IANA's tests due to unreachability.)*

DENIC agrees that providing name server addresses in unreachable or ambiguous address space fulfills no useful purpose. This check might be added to IANA's list of mandatory checks.

14. *Whether the IP addresses are on the list of reserved IP addresses.*

This test is only vaguely defined. Again, most *reserved* addresses, e.g. as specified in section 3 of RFC 3330 (less 14/8, 24/8 and 39/8), will make the request fail test (4). Properly amended this should be merged into the previous test.

15. *Whether the last octet of the name server IP address is 0 or 255.*

While there have been reports in the past about archaic software that is not yet capable of correctly handling CIDR based address allocation, including insisting on *classful* interpretation of certain addresses, DENIC does not see this test is necessary today. A warning might be issued.

16. *Whether the overall length of the name server hostname is less than 128 characters.*

DENIC does not have any idea where this random requirement originates from and thus asks this test to be dropped. Any packet length considerations can adequately be dealt with under amended test (2) above.

4 Concluding Remarks

We would like to address two additional issues found with the request for comments and the change process.

4.1 More Parties, Other Tests

The request for comments contains a paragraph mentioning, but not specifying additional tests:

> *IANA would ideally like to harmonise its technical requirements with those of other parties such as VeriSign, in order to not unnecessarily delay a request due to a disparity between differing requirements.*

The perceived presence of further *technical requirements* of unnamed third parties is of concern to DENIC. We urge IANA to research and disclose any such requirements as soon as possible and subject them to public review. TLD operators need a single reliable source of information for technical requirements and DENIC is concerned about the openness and transparency of the root zone change process unless and until all facts are published.

4.2 Root Zone Glue Policy

It is necessary that IANA document – with rationale – the current glue policy. This does not only refer to our request to rescind current test (8), but also to *ownership* of glue address records, v6 glue and packet size considerations and the current requirement to add glue records for every name server, where less glue would require fewer interactions.

5 Summary

DENIC agrees that some technical tests are applied during processing root zone change requests as precautions against adverse effects on third parties, including the general Internet infrastructure. Technical details need to refer to and follow standards and BCP documents originating from the technical community, especially the IETF.

DENIC has commented, in detail, on the list of tests provided by IANA, with the request that some of these tests, most notably test (8), be dropped or reclassified as warning level tests. In addition, some tests need to be specified in more detail and all tests should be accompanied by a rationale section explaining their need and purpose.

DENIC also has stated that it does not see the definition or execution of operational tests to be covered by the zone editor's task and asks IANA and ICANN to resolve this issue as soon as possible. This extends to the question of additional parties influencing the root zone change process by *technical requirements*.

DENIC also asks IANA to document and undertake efforts to discuss its current glue policy.

To conclude, DENIC offers to further contribute to the discussion and specification of technical checks for root zone changes and looks forward to an efficient automated procedure to process such changes.