# CENTR's Comments
## on IANA's Technical Checks Used for DNS Root Zone Changes

29th September 2006

The Council of European National Top Level Domain Registries, CENTR, thanks for the opportunity offered to comment on IANA's "Technical Checks Used for DNS Root Zone Changes".

These comments do not have the status of an official CENTR paper, but are rather a summary of all comments received during the consultation or those which are documented in official CENTR papers with regard to the IANA function, including, but not limited to
http://www.ntia.doc.gov/ntiahome/domainname/dnstransition/comments/dnstrans_comment0601.pdf
https://www.centr.org/docs/2005/04/centr-wgig-comments.pdf
https://www.centr.org/docs/2005/02/comment-icannplan.pdf
https://www.centr.org/docs/2003/03/futureiana-position.html

CENTR has always articulated that IANA should process without any delay changes to the information in the IANA database as submitted by a registry manager, provided they are properly authenticated and respect the minimum technical requirements. Such requirements should be based on clearly defined, objective, non-political and publicly available and agreed criteria. They could be implemented in predictable checks by using a public tool and the checks could be run by any third party who should be able to reproduce the results. The amount and extent of such technical checks should be inline with ICANN's mission as of Article I Section 1 of the ICANN bylaws, and go no further. According to these bylaws, ICANN's mission is "to coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular to ensure [its] (...) stable and secure operation".

With regard to the tests that IANA conducts today (v. http://www.icann.org/announcements/announcement-18aug06.htm), we further comment as follows: In general, a separation should be made for each test, clearly defining first the technical requirement and afterwards precisely describing the concrete implementation technique used to check the fulfillment of that requirement. Herewith it would be possible to discuss both of them separately. Especially the distinction between the category "mandatory requirements" and "recommendations" has not been made explicit enough in the current list. CENTR wishes that a proper process is created to manage the future evolutions of said list of requirements and checks. This future process should follow the same guiding principles of openness and community involvement.

We comment on each of the tests that IANA conducts today as follows:

1. **Minimum number of name servers.** This is a reasonable test according to the requirement of RFC 1034. It must be noted that, strictly speaking, the purpose of having "every zone to be available on at least two servers" can nowadays also be achieved by means of one IP address and anycast technology (RFC 3258). However this is not considered redundant enough: one single name server name to be resolved (regardless of how many servers are standing behind it) represents a single point of failure.
2. **Maximum number of name servers.** As clarified by http://forum.icann.org/lists/techcheck-comments/msg00005.html, the purpose of this test is to avoid truncation of DNS responses given by the root servers. However, truncation is also dependent on other factors, like the actual naming of the TLD name servers (that eases or makes message compression difficult) or the DNS query in question. Thus, this test should be subject to future improvements to take these effects into account (v. draft-ietf-dnsop-respsize-06.txt, work in progress).
3. **Hostname validity.** This is a reasonable test, but a comprehensive list of the attributes of a "valid hostname" as of STD 3 should be provided (for instance, label component and formation rules).
4. **Name server reachability.** This is a reasonable test, since it is a prerequisite for some of the following checks. However, note should be taken that transient issues could lead to a lack of responsiveness (network congestion, zone reload at the target name server, …), and hence these tests should be repeated more than once and at different times of the day before deciding to reject a change request. Additionally, care should be taken that the TLD's connectivity is tested and not that of IANA's facilities.
5. **Name server authority.** For the sake of completeness, the exact format (header and question section, v. RFC 1035, Section 4.1.1 and Section 4.1.2) of the "query for the SOA record for the top-level domain" issued in this test should be provided.
6. **Name server coherency.** This is a reasonable test.
7. **Glue coherency with hostname.** This is a reasonable test.
8. **Glue coherency with existing glue.** The aim of this test (glue coherency itself) is commendable, but the procedure is wrong, since glue coherency within the DNS is already guaranteed with test number seven. Further action can only be discussed if the current glue policy has been clearly documented, which it isn't at the moment. CENTR looks forward to commenting on the separate forthcoming IANA discussion paper on this particular practice.
9. **Serial number coherency.** Note should be taken that there are many different technologies available for content synchronization among the authoritative name servers of a TLD, some of them leading to different zone serial numbers for a zone available in the DNS for

certain periods of time. Thus, such a test should never cause the rejection of a change request, and if anything, lead to an informational message to the requestor.

10. **Minimum network diversity.** "Geographical" separation of name servers is not a characteristic that can be reliably tested or enforced; much more relevant to diversity is the "network topological" separation of name servers. However, network topological diversity must be considered under the light of anycast technology, in which a plain test for IP addresses to lie in different /24 segments might be rendered moot. This test also delivers false positives of redundancy for a single host, which could be multihomed. A test for network topological redundancy, in whichever form, should never cause the rejection of a change request, and if anything, lead to an informational message to the requestor.
11. **Name server continuity.** A complete change of the NS RRset can be a fully legitimate request in the event of a redelegation, and DNS continuity can be ensured even in the case of a complete change of the NS RRset. Thus, such a test should never cause the rejection of a change request, and if anything, lead to an informational message to the requestor.

Next, we would like to address the tests that the "implementor of IANA-approved changes to the primary root name server" conducts:

12. This test does not address any stability or security issue and thus shouldn't be performed at all.
13. This is a reasonable test and may be added to IANA's list of performed checks.
14. We cannot comment on this test unless the unspecified "list of reserved IP addresses" is provided.
15. While in the traditional classful interpretation these octet values have reserved meanings, the current CIDR obsoletes them. However some equipment is reported to still filter these kind of addresses, thus this test may be added to IANA's list of performed checks. But such a test should never cause the rejection of a change request, and if anything, lead to an informational message to the requestor.
16. The nature of this test is unclear and the threshold of 128 octets seems randomly chosen. Any concerns about DNS response truncation should be dealt with test number two (as amended by taking these comments into account). Hence, this test shouldn't be performed at all.

We would like to close these comments by pointing out that the "implementor of IANA-approved changes to the primary root name server" shouldn't perform any technical checks beyond the necessary editorial work to generate a master file conformant to the format defined in RFCs 952, 1034, 1035, 1123, 2181 and 2308. If the data provided by IANA wouldn't

allow for the root zone file to be generated and distributed, the technical checks performed by the latter should be corrected or extended as necessary. Therefore by no means should IANA seek to “harmonise its technical requirements with those of other parties”. Further, if, like this sentence seems to indicate, there is any other party besides IANA and the implementor of IANA-approved changes imposing any “technical requirements” on DNS root zone changes, it is absolutely necessary that these parties and tests be disclosed in order to ensure an “open and transparent” process, which the ICANN bylaws Article III Section 1 guarantee.