



## The Internet Corporation for Assigned Names and Numbers

21 February 2013

Dear Mr. Keith Drazek:

Thank you for your letter dated 8 February 2013, sent on behalf of the members of the Registries Stakeholder Group (RySG) and the New TLD Applicant Group (NTAG), in which implementation issues are raised on a number of topics. We appreciate the time that you spent compiling your ideas and the thoughtful considerations that you outlined for each of these topics. We would like to address the issues described in your letter.

### 1. Pre-Delegation Testing Timing

We acknowledge that the absence of an executed Registry Agreement during pre-delegation testing presents some complexities. We plan to modify the timing of the New gTLD contracting process so that pre-delegation testing occurs after the registry agreement is fully executed.

### 2. Data Escrow Full/Differential Deposits

Please note that allowing either of full or differential data escrow deposits has already been addressed in Specification 2, Section 2.2 of the revised New gTLD Registry Agreement posted for public comment on 5 February 2013. The new text reads: "*The other six days of the week, a Full Deposit or the corresponding Differential Deposit must be submitted to Escrow Agent by 23:59 UTC.*" For more information, see <http://www.icann.org/en/news/public-comment/base-agreement-05feb13-en.htm>.

### 3. Data Escrow Format

We understand the interest from a number of parties to support in the New gTLD Program the two data escrow formats being discussed by community members. The authors of draft-gould-thippeswamy-dnrd-csv-mapping and draft-arias-noguchi-dnrd-objects-mapping have agreed to merge them into a single draft. We also plan to update the New gTLD base registry agreement to reference this unified draft, therefore allowing both formats to be used.

Regarding the creation of an IETF working group, we would like to point out that there is not likely enough time to do this, given the aggressive timeline for the New gTLD Program and the IETF processes. There is an existing IETF mailing list where interested parties (e.g., gTLD and ccTLD registries) can and have been discussing the aforementioned drafts for three years. We encourage RySG and NTAG members to participate in these discussions by joining this mailing list. To subscribe to the mailing list, visit <https://www.ietf.org/mailman/listinfo/ire>.

Los Angeles  
Offices:

12025 Waterfront Drive, Suite 300  
Brussels

Los Angeles, CA 90094



USA  
Silicon Valley

T +1 310 301 5800



F +1 310 823 8649  
Washington

<http://icann.org>



#### 4. Data Escrow Criteria for Escrow Contract and Provider

We acknowledge that the process to manage the acceptance by ICANN of a New gTLD Escrow Agreement could be further specified. We are developing a process to approve the data escrow agents for New gTLD registries. We plan to publish this process shortly. As part of this process, we expect to request agreement templates from data escrow agents. This will enable them to have pre-approved templates to use in their agreements with New gTLD applicants.

We appreciate your suggestion that ICANN should also be required to sign the escrow agreement. Under the agreement as posted ICANN would approve the escrow agreement and would be designated as a third-party beneficiary. Adding a requirement that ICANN also sign the agreement would seem to create additional administrative burden on all parties and the potential for delays during the contracting process for New gTLDs. We would encourage you however to submit the suggestion, along with your accompanying rationale, to the public comment forum for the revised New gTLD Registry Agreement. We will review the suggestion in detail and consider the best course of action.

#### 5. Zone File Access Format

We recognize that converting a zone file from the standard Master File format to the format required by the Agreement would require some work from registry operators. However, our assessment indicates that this process could be fully automated and likely small in scale relative to the size of the operation that a registry manages. The format for zone files described in Specification 4, Section 2.1.4 of the Registry Agreement was developed with guidance from the Zone File Access Advisory Group in 2010. End users of the zone file that participated in the Advisory Group requested the subset of the standard Master File format as a way to simplify their processing of the zone files.

As an alternative to changing the format of the published zone files, we plan to offer in the Centralized Zone file Access System an option for registries to periodically send their zone files in DNS AXFR format. The system will convert the zone file to the format described in the Agreement. Registries that choose this option would not have to do the zone file format conversion.

#### 6. IDN Tables Format

We acknowledge the diversity of IDN table formats in use by registries and the current lack of a unified standard. However, we believe this issue has been addressed by a supplemental note to questions 15 and 44 of the New gTLD evaluation criteria: *"For variant generation algorithms that are more complex (such as those with contextual rules) and cannot be expressed using these table formats, it should be specified in a manner that could be re-implemented programmatically by ICANN."* In summary, the format specified in RFC 4290 is the preferred format, the format in RFC 3743 is an acceptable alternative, and other formats are acceptable as the last resort if the previous two do not fit the needs of the applicant, with the caveats mentioned in the supplemental note.



## 7. ICANN Reporting

We recognize there are multiple options for how an operator can operate multiple TLDs, particularly option 3 in RySG/NTAG letter (deploy a single 'instance' of their registry, with a single Shared Registry System for all TLDs). Given that each gTLD has a separate contract, it is expected that registry operators will provide monthly reports that account for all the operations related to the TLD. However, we understand that it could be difficult for some operators using the third model described in your letter to provide TLD-specific information for reporting purposes. We plan to allow those operators to include the total contact/host transactions for all the gTLDs in their platform in the monthly Registry Functions Activity Report. We understand that this would create duplicate information in several monthly reports, but it would also allow the interested parties (e.g., EBEROs) to know to which TLDs the numbers apply. We plan to update the New gTLD base registry agreement to account for this.

## 8. Pre-delegation Test Elements – DNS Infrastructure

### 8.1. Load Capacity Clarifications

We acknowledge that the load capacity tests could be further specified. We plan to release informative materials regarding the pre-delegation testing process in the upcoming weeks, including specific guidance on the load capacity testing which should address your questions on this topic.

### 8.2. "Reachability" Documentation

We understand that reachability information such as transit and peering arrangements, listing of AS numbers, and available bandwidth could be sensitive. However, this is not the only piece of information that could be sensitive, and we have put safeguards in place to handle sensitive information appropriately. Furthermore, we do not plan to request this information from every applicant. It will only be requested in special cases, such as when an on-site audit is conducted as specified in the Applicant Guidebook.

### 8.3. TCP and DNSSEC capabilities

The security issues of providing the unicast IP addresses of DNS anycast instances have been noted by ICANN, and these issues have been carefully considered while designing the procedures for Pre-Delegation Testing. The primary objectives for direct instance queries are:

- Verify DNS protocol compliance (e.g., authoritative answer, DNSSEC processing)
- Verify zone propagation delay (for compliance with the registry agreement)

It should be noted that query performance and/or query latency measurements are not an objective for direct instance queries. These are handled by applicant self-certification and/or by ICANN performing on-site auditing of load testing (as stated in the Applicant Guidebook).



Even though the pre-delegation testing provider executes its services under a strict non-disclosure agreement with ICANN, we recognize that there are providers who may be unable to allow even limited test traffic to the unicast addresses of their DNS anycast instances ("direct instance queries").

To address these issues, the current plan is to allow for query-by-proxy as an alternative to direct instance queries. This effectively means that the pre-delegation testing provider will send direct instance queries to a proxy operated by the DNS service provider. The proxy will forward the queries to the anycast instance and relay the reply back to the testing provider.

Query-by-proxy eliminates the need for the pre-delegation testing provider to communicate directly with each DNS anycast instance. For additional security, queries to the proxy may be filtered and/or rate limited if required by the DNS service provider.

We plan to release informative materials regarding the pre-delegation testing process in the upcoming weeks, including the proxy specifications.

#### 8.4. Self-Certification Template

We agree that a self-certification template would be useful. We plan to release informative materials regarding the pre-delegation testing process in the upcoming weeks, including a self-certification template.

#### 8.5. Performing Tests Against Existing Infrastructure

We agree that tests against existing infrastructure, which are designed to cause packet loss, are not appropriate for infrastructure that is being used to service existing TLD zones and live customers. The purpose of the pre-delegation technical test is to verify that the applicant has met its commitment to establish registry operations in accordance with the technical and operational criteria described in the Applicant Guidebook. Therefore, the load capacity testing is expected to be conducted on the production infrastructure. However, the subset of servers used for testing does not have to service existing TLD zones and live customers at testing time (e.g., a server could be taken out of the DNS anycast cloud during the testing period and brought back to the cloud thereafter).

We greatly appreciate your feedback. Thank you for your participation in ICANN's multi-stakeholder model.

Best regards,

A handwritten signature in blue ink, appearing to read "Akram J. Atallah".

Akram J. Atallah  
Chief Operating Officer, ICANN