New gTLDs

Issues with the „New gTLD Agreement“

for v.3 of the ICANN proposal

2009-11-23

Richard Wein
CEO, nic.at

1 Document Overview

This document provides an analysis of the current draft version of the “New gTLD Agreement”, particularly with regards to the technical and commercial feasibility of registry operations for smaller new gTLDs (“community TLDs”).

This document does not address the issues around the financial risk of the proposed application process itself, but focuses on issues that arise from the technical and administrative requirements set in the proposed draft.

2 Format of the Escrow Data (minor)

The data format of the Escrow specification implies a certain registry structure. For example, many existing, long establishes registries currently have some differences, particularly in:

- Host Objects: Many registries do not use host objects, but rather use the host attribute mechanism of EPP (no Nameserver handles).
- Contact Transfers: Many registries do not allow the transfer of contacts

It is assumed that particularly community TLDs (for example, “brand” type TLDs) might not support all of the described object types. The specifications already hint at the fact that some registries might not support all of the object types (“supported object types”) – however, the specification should be clearer about which of the reports are definitely required.

We specifically acclaim that daily reports can be send via “authenticated email”, since daily manual reporting in written form would pose an unnecessary burden on registry operators as well as ICANN.

3 SLA Performance – Monitoring

The current draft of the Agreement is contradictionary whether the Registry Operator or ICANN is to operate the “sensors” described in SPECIFICATION 3. Section 1 and Section 2 seem to imply that the Applicant is to operate the nodes, and send reporting to ICANN, while “Listing of Probes” in SPECIFICATION 6 explains that ICANN provides a list of probes, indicating that ICANN would operate the probes.

Because of economy of scale, and particularly equal treatment of Registries, operation of such probes by ICANN is the preferred choice.

Putting the burden of operating the indicated high number of probes to each and every Registry Operator would

1. create monitoring data that cannot be compared among different registry operators / TLDs
2. essentially make the operations of smaller, community driven TLDs commercially unfeasible, and put unfair advantage at large, established gTLD operators with a huge infrastructure.

4 SLA Performance – EPP monitoring

The requirements of 99.9% availability **including planned maintenance** makes the provision of such registries unfeasible for smaller community TLDs (below <100.000 domain names, and not considering ramp up costs!).

In addition, compared to DNS SLA performance, putting such high requirements to EPP interfaces seems unreasonable – while DNS performance obviously is important for the technical functionality of a registry system, availability of the EPP interface is of much less concern to Registrars and Registrants.

Also, many large, established ccTLDs have run their business successfully with planned maintenance windows (for example on Saturday/Sunday) without any complaints from Registrars, given that the planned maintenance is announced well in advance.

To make the operations of a registry system feasible for community TLDs, we suggest that ICANN revisits the SLA requirements, and we propose two options:

1. **99.5%** Availability of EPP interface, **including** planned maintenance per month (giving about 3 hours of time each month to perform planned maintenance – which is typically enough for a well-planned maintenance). ICANN should allow Registry operators to request additional planned maintenance time in exceptional situations.
2. **99.8%** availability of EPP interface, **excluding** planned maintenance per month (allowing for about 80 minutes of downtime each month). Planned maintenance must not be considered for that availability.

Also, other options are possible – for example extending the time window that is used for SLA calculations – however, the currently proposed availability of 99.9% per month, including scheduled maintenance is contrary to the requirements of the industry, puts an immense technical effort at prospective Registry Operators, and again puts unfair advantage to operators of existing huge gTLDs – particularly because the effort of providing high availability should rather be invested in achieving 100% uptime for the DNS, rather then the Registry system itself.

For example, the Austrian Registry (.at, ~900.000 domains) has operated with an availability of the EPP interface of 99.95% for the first half of 2009, excluding planned maintenance, and was above 99.9% for each individual month. However, including planned maintenance on a per-month basis, however, has reduced the availability to 99.65% for the month in which a major upgrade to the database storage system has been performed – something that is administratively and commercially unfeasibly to perform in the required 43 minutes. The maintenance was announced well in advance, and was performed well within the time window. No complaints were received from registrars.

Therefore, we urge ICANN to reconsider the SLA levels for the EPP interface, giving well-established medium sized registry operators at least a chance to compete with industry leaders, particularly for smaller, community-based new TLDs.

5 DNS SLA (SPECIFICATION 6)

We agree with the general requirements that DNS must be available for **100%** of the time. However, for similar reasons as outlined above, we disagree with the requirement that every single IP address listed for a TLD must be available for **99.9%** of the time per month, and we do also think that this requirement has a risk of reducing the overall service availability in case of systematic architectural problems, particularly for the following reasons:

- The availability of 99.9% per IP address can only be achieved by creating Anycast networks for each of the public IP addresses (a simple local DDoS attack would otherwise be enough to take out the public IP address completely – this is mostly out of control of the Registry Operator).
- However, for reasons of diversity, Registry Operators typically want to mix different technologies, to achive an higher overall availability – particularly mixing Unicast and Anycast IP addresses. By putting the proposed SLA requirement on all IP addresses ICANN prevents Registry Operators from being able to do so (see above), and therefore puts the whole TLD at risk in case that a architectural flaw (for example in Anycast technology) is discovered.

- Also, the “de facto” requirement of Anycast for each of the public IP addresses would create an additional demand for address space in IPv4 and AS numbers – essentially at least one /24 and one AS per listed IP address.
- The only way to “escape” from long-running DDoS attacks on Unicast nodes would be to change the public listed IP address of the affected TLD nameserver. To achieve that within the required 43 minutes, ICANN would also need to be able to apply that change to the root zone within those 43 minutes – something that is not possible with the currently established administrative processes.

Therefore, we urge ICANN to reconsider the DNS SLAs, for example by requiring:

- 100% overall availability for the TLD (defined as that at least one public IP address of the DNS network must be reachable)
- 99% availability for every listed IP address (allowing for ~7 hours to apply reasonable countermeasures like increasing upstream bandwith, implementing adaptive fitering in the worst case of a sustained DDoS attack)
- or, even, a “graded” model, for example (because the availability “multiplies” among the number of nodes):
  - 2 public IP addresses provided: 99.9% per node
  - 3 public IP addresses provided: 99.8% per node
  - 5 public IP addresses provided: 99.5% per node
  - 7 or more public IP addresses provided: 99% per node

Reasoning: The current SLA requirements would make it very attractive for new TLDs to only provide e.g. two Anycast-based nameserver ip addresses for a single TLD, and nothing else – because adding “weaker” unicase nodes (and therefore increasing the diversity of the network) puts the operator at risk that one of those “weaker” nodes might not fulfil the tough SLAs. That risk becomes greater – we don’t think that this is the ultimate goal of ICANN.

6 Number of “probes” for EPP

As outlined above, we consider the EPP interface much less important than the DNS interface, particularly for smaller TLDs. Therefore, we urge ICANN to reconsider the number of probes required for the EPP testing, and propose that ICANN reduces that number to **2 nodes**.

The number of probes currently indicated in the draft would only make sense if ICANN would operate the probe themselves, and therefore allow for economy of scale among different Registry Operators.

We are also concerned about probes operated by an existing Registry Operator of gTLD services – a neutral third party would be preferred.

7 Number of “probes” for DNS

For the same reasons as outlined above, we consider the number of DNS probes unnecessary high, particularly for smaller TLDs.

The required number of **20 probes** makes only sense if those probes are shared, or operated by a neutral third party (for example, similar to RIPE’s DNSMON service). If the probes are to be operated by the Registry Operator itself, we believe that **5 probes** should be enough for smaller new TLDs.