Saint Quentin en Yvelines, November 20, 2009

Comments on the new gTLD Draft Applicant Guidebook v3

Contents

1. Introduction and statement of Interest

AFNIC is a not-for-profit, multistakeholder organization founded in 1997, managing the French country-code top level domains *.fr, .re, .tf, .wf, .pm* and *.yt*. AFNIC is a member of ccNSO and a founding member of CENTR, the European regional organization of ccTLDs gathering 57 ccTLD managers.

Recently AFNIC, in cooperation with CORE, was selected by the City of Paris to provide back-end registry services for the *.paris* TLD project. In the context of future new gTLD applications, AFNIC may also be involved with providing services and support to other applicants.

We welcome this opportunity to comment on version 3 of the Draft Applicant Guidebook and thank ICANN staff for the amount of effort put into the various documents. Our comments aim to provide constructive advice in order to reinforce fairness, effectiveness and simplicity in the process, so that delays can be reduced and applications accepted in the near future.

2. Continued delays in the new gTLD application timeline: mitigating the detrimental effects on prospective applicants and ICANN's legitimacy through the adoption of an incremental approach

The absence of clear and predictable deadlines for the application process is highly detrimental to applicants and their partners. As a not-for-profit organization supporting prospective and potential applicants, AFNIC is concerned that the current expenses and investments needed on new gTLD projects can no longer be balanced with defined expectations of cost recovery.

AFNIC has closely followed the discussions and debates on the so called overarching issues which are leading ICANN to delay gTLD applications once more. We do recognize that specific types of gTLD applications may cause acute problems which motivate the devising of appropriate safeguards. However, we believe there are also specific categories of gTLD projects which will not and cannot cause such problems. Besides, such projects are currently falling victim to collateral damage caused by ICANN's imposition of continued delays and unnecessary rules.

For instance, recognized social-purpose gTLD projects, such as those of capital cities or cultural and linguistic communities, can provide immediate proof of social and economic benefit to their community, guaranteed protection against Intellectual Property abuse, and negligible impact on the DNS root due to their limited number. In particular, the governance structure and policies that prospective operators of such TLDs would have to design in order to secure the support of their relevant public authorities, added to the legal framework to which these authorities are accountable, can clearly and convincingly show how abuse would be improbable if not impossible altogether.

Additionally, we would like to highlight the fact that delays imposed on the new gTLD process currently harm ICANN's credibility and, thus affect its legitimacy. This is why we urge ICANN to consider new pragmatic approaches while clarifying the timeline of the process. Most importantly, we recommend ICANN adopt an incremental approach to the processing of new gTLD applications. Instead of imposing a one size-fits-all set of rules and a uniform process to all prospective new gTLD applications, ICANN should consider differentiating applications based on the nature of their support, governance, and policies. For ICANN, such an incremental approach would combine the advantages of effectiveness and security by opening a first gTLD applications window in the near future, while still allowing for the design of appropriate policies for more problematic types of projects.

In any event, we believe that gTLD applications should start to be accepted by the end of the third quarter of 2010, at the latest. Moreover, in compliance with its accountability commitments, we believe that ICANN should back its assurances that it will open new gTLDs with a penalty system: in the event of the gTLD application timeline significantly shifting again, ICANN would be bound to lower its application fees.

3. Capital city gTLDs applications: required documentation of support or non objection needs more precision

In DAG v3, capital city names such as Berlin or Paris have been recognized as belonging to a separate sub-category of geographic names. This is a step forward on the way to their protection. However, as we and others understand the current version of the DAG, it is still unclear whether the applicant for a capital city TLD would need documentation of support or non-objection from all relevant governments or public authorites in the capital's country, as well as in other countries where a city of the same would exist.

It should be clearly stated that in the case of "*an application for any string that is a representation, in any language, of the capital city name of any country or territory listed in the ISO 3166-1 standard*", it would be sufficient for the applicant to provide evidence of support or non-objection from the national government relevant to that capital city. The applicant would therefore not be required to document support or non-objection from countries which could happen to have a city of the same name.

4. The Continued Operations Instrument: not always appropriate, nor necessary

The Continued Operations instrument layed out in Specification 8 of the draft Registry Agreement is described as a financial instrument (cash escrow or letter of credit) to ensure continued operations of the basic registry function for a period of 3 years.

We remind ICANN that this safeguard may be irrelevant in the case of a gTLD operated directly by a public authority such as the City of Paris. Indeed, as a public authority comparable to a state in the US, it cannot legally default. In addition, the provision of such an instrument would constitute a blatantly unjustifiable use of taxpayer money.

We therefore recommend ICANN replace this financial instrument with a form of commitment by a third party (such as an industry player) to ensure continued operations of the Registry for 3 years, at its own expenses, in case of failure of the Registry Operator.

5. Registration Data Publication Service: inapplicable in France

Specification 4 of the Revised Proposed Draft New Registry Agreement requires in Section 1.1.2 that Registry operators provide detailed information about the registrants including personal information.

We would like to inform ICANN that this provision is not applicable under the French legal framework. Indeed, under Act N°78-17 of January 6, 1978 on *Data Processing, Data Files and Individual Liberties* amended by the Act of August 6, 2005 *relating to the Protection of Individuals With Regard to the Processing of Personal Data*, personal information of individuals (such as name, address, telephone number and email address) ought to be protected and cannot be published without formal consent. Without this consent, personal data of a registrant can only be disclosed under stringent terms in the context of judicial proceedings or a summary order issued by the relevant authorities.

Incidentally, ICANN Staff have declared in the past that provisions such as those approved for the *.tel* Registry Agreement may be acceptable. We urge ICANN to commit to this policy in writing by updating the DAG accordingly, and make the option available to new gTLD Registry Operators

6. Issues around the proposed new Registry Service-Level Agreement
(in collaboration with nic.at)

SLA Performance Monitoring

The current draft of the Agreement is contradictory on whether it is the Registry Operator or ICANN that operates 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. 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.

To avoid discriminatory measures, and for the sake of the efficiency generated by economies of scale, operation of such probes by ICANN should be the preferred choice. As the registry for *.fr*, AFNIC has contracted with a third party to provide monitoring of some of its services. We are willing to share feedback on potential contractors and their services. We would also recommend lowering the total number of probes.

Newly defined SLAs unfair towards small projects: revert to v2 of the DAG

The DAG version 2 included service levels for DNS availability and registration data publication service. Without justification (as far as we know), version 3 introduces drastic changes by setting very high service level expectations and introducing service level for EPP services.

These changes introduced in version 3 create unnecessary burden to small community-driven projects and are unnecessary. It must be noted that ICANN's remit is not to create a market performance standard but to ensure that minimal requirements are set to ensure security and stability of the Internet.

It must be stressed also that contrary to incumbent players, new gTLD Registries will have very strong incentives to provide high-quality EPP services if they want to attract registrars. It is therefore unnecessary for ICANN to interfere with competition.

Finally, this set of service levels, while relevant to the business of top level domains we currently know, may soon be outdated by the new business models expected to flourish in the context of the new gTLD process. Maintaining version 3 of the specification will therefore either constitute a barrier to innovation or soon become inefficient.

For all aforementioned reasons, we recommend to revert to version 2 of the DAG in this section and focus on DNS Service availability (100%) and RPDS availability (99% being more than enough since RPDS is NOT critical to Internet security and stability).

DNS Service Levels raise security and stability issues

As stated before, we agree with the general requirements that DNS must be available for **100%** of the time. However, in addition to the reasons listed above for removing the DNS Name Server availability SLA, we want to stress the potential drawbacks of requiring that every single IP address listed for a TLD must be available **99.9%** of the time. Indeed, such a requirement carries a risk of reducing the overall service availability in case of systematic architectural problems, particularly for the following reasons:

- The 99.9% availability for each IP address can only be achieved through 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 in order to achieve higher overall availability, Registry Operators typically mix different technologies – particularly Unicast and Anycast IP addresses. By imposing the proposed SLA requirement on all IP addresses, ICANN prevents Registry Operators to keep following their diversity strategy, and therefore puts the whole TLD at risk in case of an architectural flaw being discovered (for example in the Anycast technology itself).
- Also, requiring "de facto" Anycast for each public IP addresses would create an additional stress on IPv4 address AS numbers demand – 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.

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" Unicast nodes (and therefore increasing the diversity of the network) puts the operator at risk that one of those "weaker" nodes might not fulfill the tough SLAs. That risk becomes greater – we don't think that this is consistent with ICANN's core values.

We therefore urge ICANN to remove, or at least reconsider these new SLA standards. Suggestions for amendment could be:

- 100% overall availability for the TLD (defined as "at least one public IP address of the DNS network reachable at all times")
- 99% availability for every listed IP address (allowing for about 7 hours to apply reasonable countermeasures like increasing upstream bandwidth or implementing adaptive filtering in the worst case of a sustained DDoS attack)

- or, even, a “graded” model, for example (because the availability “multiplies” with 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

Another aspect of this DNS SLA is the requested update time of 15 minutes. The arguments described above (sub section “Newly defined SLAs unfair towards small projects: revert to v2 of the DAG”) fully applies here as well. In addition, we believe that this expectation creates an unnecessary risk for the security and stability of the Internet.

First, there is the obvious Fast Flux issue: should a registry operator wish to implement the SSAC recommendations, this service level may limit its ability to do so.

Then as far as we know, there is currently no registry system in production that has both high frequency zone file updates as well as a significant number of DNSSEC signed delegations. Moreover, we understand that some in the technical community are concerned with potential instabilities that may arise in such situations.

For these reasons, we recommend to remove this dimension of the SLA, or at least to set the minimum frequency at several hours.