

Comments on concerns raised by ccTLD Document 46

Version 1.0

Council of European National Top Level Domain Registries

28 February 2003

In Document 46 lodged for the ITU ccTLD Workshop of March 2003, Nominum analyses some technical protocol compliance of the network of name servers that provide the authoritative information for ccTLDs. We consider that whilst the figures provide a reasonable picture, it would be easy to jump to false conclusions that give an incorrect impression on the technical stability of the ccTLD name system.

Summary of Nominum Paper

Nominum is a company substantially involved with providing consulting services relating to the DNS, as well as selling commercial name server software designed to compete with products like BIND. It has also recently provided commercial name server outsourcing services to ccTLDs.

In the report, a number of categories of technical non-compliance have been tested for and tallied. It assesses performance by many ccTLDs to be surprising and disappointing under the testing areas. The report doesn't give indications as to the identity of these non-compliant ccTLDs, or rationale why these circumstances may exist.

Points of Clarification

In response to particular sections:

- ?? *Parent/Child mismatches* – Parent and child mismatches will always be an element during the transition from one set of name servers to another. With proper planning this has no impact on DNS performance, as the report identifies. The only appropriate way to effect a successful change of name server delegation is for the child to reflect the change, and then to request the change be made by the parent. It is important that the root name servers are updated by IANA in a timely manner to reflect changes that ccTLD operators need to make.
- ?? *Recursive Servers* - Whilst perhaps authoritative-only name servers are ideal for zones, considering the role the ccTLD Manager may have in smaller countries, it is understandable why recursive name servers are offered. Often run by academic networks that offer one of the few central computing facilities in the country, they provide a service to the local community in providing their only DNS forwarder. It is in the local Internet communities interest to offer a mixed role compared to that of a pure ccTLD manager.
- ?? *Open Zone Transfers* - We generally agree zone transfers should be denied, although that is a matter of local policy from country to country. Some countries with limited means rely on the support of third-party volunteers over whom they can not exert policy control over – making zone transfers

available.

- ?? *Fingerprinting* and diversity - Until very recently, the two key choices ccTLDs had was between BIND 8 and BIND 9. Whilst there have been some issues with BIND 8, BIND 9 has not proven to be a clear replacement choice. ccTLDs have considerable operational expertise in operating and testing name servers and have evaluated many of the different options available. BIND 8 has to many proven to be more robust, and gives higher performance than BIND 9. As is good practice with all software, ccTLD Operators are aware they need to take precautions to ensure security and limit any potential problems, and actively monitor and identify new faults.
- ?? *Monitoring* - Many ccTLDs and other parties have extensive monitoring systems continuously evaluating performance, and checking for service faults.
- ?? *Service Level Agreements* – The Nominum document proposes that binding agreements (“service level agreements”) are essential between “the zone owner” and entities providing name server services. However, such agreements are only appropriate between the ccTLD operator and its service providers. These may not be appropriate for ccTLDs who rely on volunteer services, and formalized agreements with strict standards may be beyond their needs.

It is important to realize there are no service level agreements at the top ('root') level, between IANA/ICANN and the root name server operators.

- ?? *Distributed Denial of Service Attacks* – Denial of service attacks represent a serious threat which frequently changes and requires preparation and rapid response. The lack of appropriate defence by ccTLDs to a major denial of service attack is merely unsupported speculation.

The ccTLD name server operators are working with root name server operators on collaborating communication on attacks, and preparing for other potential risks.

Additionally,

- ?? In setting best practice standards for operating name servers and other DNS functions, there must be careful consideration of the means available in each country. Some countries have extremely limited networks, and onerous obligations are perhaps unnecessary and may require telecommunications infrastructure to be moved out of the country to be fulfilled. We believe forcing countries to cede their fundamental operations for these reasons is undesirable.
- ?? Some differences represent broad policy diversity between ccTLDs, and these policy represent the differing expectations of local Internet communities. By enforcing strict rules on how to operate ccTLDs, it restricts the capacity for ccTLDs to improve and innovate.

Summary

The ccTLD community considers the role of operating a stable DNS paramount.

We have a track record of reliable service. We recognize there are places for improvement and areas where more work can be done, but there have been no fundamental service disruption in the operation of major ccTLDs.

ccTLDs have demonstrated their responsibility in running their services in a robust and accountable way. Whilst Europe is one of the most technically accomplished regions in DNS deployment, and for the most part are not reflected in the technical faults in the Nominum report, we recognise diverse circumstances have lead to the current worldwide picture that needed to be explained.