INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR	**ccTLD Doc 51 Rev.1**
STUDY PERIOD 2001-2004	**Original: English**

Workshop on Member States' experiences with ccTLD

Geneva, 3-4 March 2003

DOCUMENT FOR ccTLD WORKSHOP

Source: CENTR

Title: About the Administration of the Internet Domain Name System

---

About the Administration of the Internet Domain Name System

Editors: Richard Francis, Nigel Roberts, Stephan Welzel, Marianne Wolfsgruber, Kim Davies

28 February 2003

Contents

Contact:	CENTR secretariat	Tel:	+44 1865 332400
	Council of European top level domain	Fax:	+44 1865 332401
	registries	Email	secretariat@centr.org
	Oxford, United Kingdom		

Abstract

This paper describes the Council of European National Top-Level Domain Registries (CENTR), and the view of CENTR members toward the administration of the domain name system. The ccTLD managers in Europe have provided a high quality, dependable infrastructure service since the early days of the Internet. The services provided to the community are based on the principle of self regulation, as demonstrated by CENTR's documentation of best practices for ccTLD managers. The legitimacy of a ccTLD manager derives from the local Internet community (LIC) to which the respective country code has been assigned.

Any change of ccTLD manager is an issue with policy implications as well as potentially having significant impact on technical stability. It requires the broadest possible dialogue within the LIC. Only the LIC operating under local legal jurisdiction , can guarantee that the needs of the community are met when appointing a new or replacement ccTLD manager. Any change must be carried out in a responsible manner, considering the needs of global stability.

The IANA ccTLD function is essential for the technical stability of the DNS, and must to be carried out by a body which has the complete trust and acknowledgement of all parties concerned. Such a body must not deal with policy, rather only maintaining the official record of the data connected to the management of the ccTLDs.

In all European countries the ccTLD manager has a local presence. Therefore the relationship between the ccTLD manager and the respective government is a purely local issue. The global nature of the Internet creates only a few (mostly technical) DNS issues that require global coordination. To provide for a forum for this global coordination, ICANN was created. The governments, embodied as the Governmental Advisory Committee (GAC), play an integral role within ICANN. CENTR's members encourage the GAC to engage in a closer dialogue with the ccTLDs on ICANN's performance in delivering a well functioning IANA .

CENTR considers an effective global framework is important in ensuring stability and responsibility within the global domain name system. We are optimistic progress is being made, and that through the efforts of all stakeholders we will continue down a productive path toward developing and refining this framework. We submit our comments as a step toward constructively working through these issues.

Introduction

CENTR members welcome the opportunity of contributing to this workshop arranged by the ITU Telecommunications Standardisation Sector (ITU-T). We are pleased to present an overview of some of the work being done by CENTR in matters concerning the Internet Domain Name System. CENTR members are grateful for the opportunity to exchange information with a wider range of contributors.

About CENTR

http://www.centr.org

ccTLD managers in Europe have played, and continue to play, a pivotal role in ensuring the robust operation, technical stability and interconnection of the Internet Domain Name System since 1986 and the earliest days of the Internet.

In 1998 European ccTLD managers formed the Council of European Top Level Domain Registries (CENTR) to encourage the development of Policy and Best Practice for European ccTLDs in a stable, integrated and coherent forum. The membership of CENTR has grown to encompass most European ccTLD managers.

CENTR believes that the sharing of experiences between European ccTLD registries which it has engaged in since 1998 has added significant value to the European and global Internet communities. CENTR members continue to work together to ensure the ongoing success of the Internet and is committed to the principle of industry self-management.

Background

In October 2002, the ITU Plenipotentiary issued resolution 102 on the Management of Internet domain names and addresses.

Resolution 102 recognizes that the global information infrastructure is of crucial importance as engine for growth in the world economy and that the private sector has the crucial role in ensuring the sustainable development of the Internet for the benefit of all. The resolution also encourages the ITU to take an interest in ongoing international discussions on particular Internet issues.

The Internet Addressing System

Shaped and nurtured by private initiative, the Internet has become broadly used and highly valued. It is today being utilised for communication and information exchange in many different areas, including commercial activity (e-commerce). Consequently, this contributes significantly to the economic and social well being of people all over the world.

As the addressing system (domain names and IP-addresses) is an important part of the Internet, its impressive development emphasizes this system's importance. At the core of the system are the so-called IP-numbers which serve to direct all Internet traffic and which thus deserve the highest attention by anyone with an interest in the functioning of the Internet. However, the DNS which was developed later further enhanced the Internet's usability and acceptance.

CENTR members believe that the management of the DNS is most efficient and productive, when the lead is being taken and kept by self-regulating institutions which, at the same time, are aware of the general importance that is now being attached to the DNS. Such self-regulating bodies, because of their immediate relationships with all interested parties, are best able and most willing to take on and adjust to the challenge which derives from the high speed of the DNS's ongoing development and the highly complex needs and demands of all Internet users. CENTR members appreciate that among the Internet users are by now also public administrations as the development of methods to deploy public services via the Internet is, encouraged by governments, under way in many countries.

In this spirit of self-regulation and in consultation with and for the benefit of all concerned parties, ccTLD managers ensure a secure and reliable management of ccTLDs within a clear, consistent and predictable policy framework .

Furthermore, experience demonstrates that with regard to the administration of a ccTLD it is both necessary and desirable to pay the foremost attention to local needs and circumstances. This can

only be guaranteed by the involved parties on a local level. For those governments which have a particular interest in the management of the ccTLD assigned to their respective territory, CENTR believes that local fora are the most appropriate.

In view of this, CENTR members are convinced that global institutions like, for example, ICANN with its currently evolving ccTLD Supporting Organisation only can and shall have a strictly limited role in developing policy that affect ccTLD registries.

ROLE AND FUNCTION OF ccTLD MANAGERS

To ensure that the requirements as outlined above be met CENTR has developed Best Practice Guidelines for ccTLD Managers which were adopted by the General Assembly on 10 May 2001 and can be found at :-

http://www.centr.org/docs/legal/best-practice.html

Legitimacy of a ccTLD manager

As highlighted in CENTR Best Practices, legitimacy of a ccTLD manager derives from the Local Internet Community of the territory to which the respective country code has been assigned.

The Local Internet Community comprises all involved parties, including both the private and the public sector.

The role of ICANN as a private, not-for-profit institution coordinating specific DNS functions and technical parameters for the benefit of the Internet and its users as a whole is generally accepted and supported by ccTLD managers. It needs, however, to be clearly stated that the desires and decisions of the Local Internet Community of any given territory must have priority over any recommendations issued by ICANN. This is particularly important as local law affects the administration of a ccTLD. Examples of this might be data protection or privacy laws.

Registrant Policies to ensure a fair and stable system

The ccTLD manager must be equitable and fair to all eligible registrants that request domain names. Policies as to which domain names can be registered, how registration requests are processed, and who is eligible to register domain names must be defined by the ccTLD Manager in consultation with the Local Internet Community. The ccTLD manager's policies must be documented, available for public inspection, and transparent to the Local Internet Community. Specifically, the registration of domain names should be based on objective criteria that are transparent and non-discriminatory albeit in detail policies and procedures will vary from country to country due to local customs, cultural values, local policies and objectives, law and regulations.

Change of ccTLD Manager

A change of the ccTLD manager occurs when the current manager ceases its responsibilities and a replacement is therefore required.

In the course of such a change, the designation of a new ccTLD manager is, obviously, an issue with policy implications as well as potentially having significant impact on technical stability. Since these are local matters, they will require the broadest possible dialogue with and within the Local Internet Community. Once an agreement on the new ccTLD manager is reached instruction will be given to IANA to make the necessary changes.

Only the Local Internet Community operating within the legal system of the local community can guarantee that the needs of the community are met when appointing a new or replacement ccTLD manager.

However, duties also attach to the function of ccTLD manager and the corresponding Local Internet Community. Such duties include taking account of the stability of the global Internet, as well as responsibility to and service for Internet users both locally and globally.

Any change of ccTLD manager must take these responsibilities fully into account. Existing ccTLD managers must not be subject to arbitrary action, nor have discriminatory practices, policies or procedures applied by governments or other public authorities.

As the ccTLD manager should be established in the respective territory it is automatically subject to the local law and therefore every change of ccTLD manager will simply be a local issue, where global authority is neither needed nor desired. In this context, local law provides the framework for the powers and responsibilities of the government.

The IANA ccTLD related function

The IANA-ccTLD function must to be carried out by a body which has the complete trust and acknowledgement of all parties concerned.

Such a body must not deal with policy, which instead should be within the scope of responsibility of a separate IANA-ccTLD policy body. Such separation of the policy creation for the IANA and the operational role is particularly necessary in the light of some recent experiences with the current IANA.

The processes and structure of the body empowered to action changes in the ccTLD database must incorporate some form of independent quality auditing, and a complete audit-trail of all operations must be maintained. Such auditing could be carried out within the context of an agreement between the body carrying out the IANA ccTLD function and the ccTLD manager.

In this concept the IANA function has no role in quasi-judicial determinations, but keeping the only official record of the data connected to the management of the ccTLD.

CENTR has made submissions to the US Department of Commerce making detailed recommendations on the future operation of the IANA which was put before the General Assembly in Frankfurt 27-28 February 2003. The submissions in their current form are available at
http://www.centr.org/news/Letter-future-IANA.pdf

Technical Stability

CENTR members are heavily involved in promoting a stable domain name system.

This is a role the industry considers to be of paramount importance.

Whilst we have a track record of reliable service, we nevertheless constantly work on advancing the quality of both our technical and administrative services. We recognise there are always ways to improve our service, but note that for many years there has been no fundamental service disruption in the operation of any major ccTLDs.

Whilst Europe is one of the most technically accomplished regions in DNS deployment, we are for the most part are not reflected in the technical faults in Document 46 of the ITU ccTLD WS, March 2003. (See attachment for information pertaining to this document)

ROLE OF GOVERNMENT

Relationship between ccTLD Manager and the corresponding Government

Where the ccTLD manager has a local presence in the territory to which the country code is assigned the manager is subject to local law and its relationship with the local government is simply a local issue. The creation of any global authority over the ccTLD is then not needed nor would it be in the country's interest as in this situation the government, as part of the local legislation process, obviously has already legislative power over the ccTLD manager.

Governments on a global level

Every party significantly interested in the management of the DNS must take account of the fact that each and every action on that management has the potential to adversely affect the stability not only of the operation of a ccTLD locally but also of the global Internet as a whole. The globality of the Internet, on the other hand, also means that there are a very few (mostly technical) issues related to the DNS that require global coordination. To provide for such global coordination ICANN has been created and CENTR members are hopeful that a reformed ICANN involving participation of ccTLDs will manage to foster this coordination. CENTR members believe that ICANN comprises all involved parties and appears to have best potential (despite some disappointments in the past) to allow for the building of global consensus on the broadest possible basis.

The governments are – within ICANN´s Governmental Advisory Committee – an integral part of ICANN and thus play a significant role in the international coordination and consensus-building already. To enhance the ICANN-GAC's involvement even further, CENTR members explicitly encourage GAC to engage in a closer dialogue with the ccTLDs relating to the ICANN's performance in delivering of IANA .

The environment for gTLDs is different to that from ccTLDs and , by definition, is global, not local. Although companies running gTLD registries are typically based in a single country, they are global in their scope and services and affect stakeholders worldwide. In this regard a somewhat broader international coordination role is probably advisable, even more so as it might encourage the development of an environment for the introduction of new gTLDs that take the interest of all stakeholders into account.

CONCLUSION

The Internet has become the amazing success that it is today due to self-regulating mechanisms which flexibly and speedily respond to the needs of Internet users. As part of such self-regulating systems governments have played and will no doubt continue to play their part, such as within the Governmental Advisory Committee. Naturally, governments have the possibility to give voice to their considerations through their own legislative processes.

In the spirit of self regulation a stable and secure environment has been created for both the Local Internet Communities and the global community In view of all of this, there is neither a need nor a common demand for significant or even fundamental changes to the management of the DNS. CENTR members are therefore convinced that the DNS and thereby the Internet as a whole is best served if the well tried current balance between the public and the private sector remains unaltered in the main.

February 2003

Attachment 1

Comments on concerns raised by
ccTLD Document 46

Council of European National Top Level Domain Registries
Version 1.3

28 February 2003

Document 46 lodged for the ITU ccTLD Workshop of March 2003, 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.

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. ccTLDs have continuously worked to improve the performance of IANA in this respect.

- *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-parties over whom they can not exert substantial policy control over, thus making zone transfers available.

- *Fingerprinting* and diversity - Until very recently, the two key choices for ccTLDs had been between two versions of name server software BIND – versions 8 and 9. BIND 9 has not proven to be a clear replacement choice for BIND 8. ccTLDs have considerable operational expertise in operating and testing name servers and have evaluated 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 Agreement*s – The 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. Formalized agreements with strict standards may be beyond the needs of ccTLDs.

  It is important to realise 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, monitoring 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 collaborating with root name server operators on matters such as denial-of-service 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 in 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 report, we recognise diverse circumstances have lead to the current worldwide picture that needed to be explained.

———————