

**DOCUMENT FOR ccTLD WORKSHOP**

**Source:** Co-Chairmen  
**Title:** Draft Summary

---

The relationship between government and operator of the corresponding ccTLD may be formal or informal in nature.

In many cases, domain names come under the provisions of a general telecommunications law and the government exercises its formal powers, or its informal influence, through the ministry of communications or the telecommunications regulator. The appropriate government authority may supervise the activities of the ccTLD operator and approve their pricing policy if there isn't a competitive registry-registrar model.

In other cases, previous informal arrangements are being clarified and/or formalized, under the sponsorship of the government, and in consultation with all concerned parties, because it is held that matters related to the administration and operation of the ccTLD are of public interest. The public interest arises from the growth of the Internet and its use to facilitate electronic commerce and the information society.

It appears that there would be interest in, and scope for, agreeing framework "best practices" in certain areas. Indeed, WIPO has developed such for dispute resolution.

ICANN states that it has a well-defined mission: to coordinate the administration of the Internet's systems of unique identifiers (domain names, Internet protocol addresses, and protocol port and parameters numbers). In this context, ICANN also develops global policies as reasonably necessary to its main technical mission. Governments and distinct economies participate in ICANN through the Governmental Advisory Committee (GAC).

In simplest form, states ICANN, its core mission is the stability of the Internet's naming and addressing systems. ICANN operates according to a Memorandum of Understanding with the U.S. Department of Commerce. Under the MOU, ICANN handles matters relating to the domain name system's top-level domains, including any changes to be made to the DNS Root Zone File, subject to the final approval of the DoC. Under this agreed framework, a request for delegation, redelegation, authoritative name server changes, and so forth, are submitted to and processed by ICANN.

ICANN has recently undergone a significant reform. Under the reformed structure, there will be a Country Code Names Supporting Organization (ccNSO) directed to matters of global policy and

---

**Contact:** Richard Hill

Tel: +41 22 730 5887

Fax: +41 22 730 5853

Email: [richard.hill@itu.int](mailto:richard.hill@itu.int)

**Attention:** This is not a publication made available to the public, but an **internal ITU-T Document** intended only for use by the Member States of the ITU, by ITU-T Sector Members and Associates, and their respective staff and collaborators in their ITU related work. It shall not be made available to, and used by, any other persons or entities without the prior written consent of the ITU-T.

other issues affecting ccTLDs. Work towards the structure of this supporting organization is nearing completion, and will be finalized by the next ICANN Board meeting in late March 2003.

Country-Code Top-Level Domains, or ccTLDs, were initially delegated by Dr. Jon Postel with the objective of enabling local Internet communities worldwide to develop their own locally-responsive and -accountable DNS services, and to encourage all parts of the world to 'get online'. Initially, from the mid-1980s to the mid-1990s, ccTLD registry responsibilities were typically delegated to Internet pioneers, often from the academic or research communities. In 1994, Dr. Postel published the basic policy and technical requirements for TLD delegations, redelegations, and operations in a document known as RFC 1591.

Today, in a vastly more complex global Internet environment, ICANN states that it carries on Dr. Postel's work by seeking to institutionalize and document the framework for ccTLD delegations, consistent with the existing published policies. In this role (known as the IANA function"), ICANN has the responsibility to investigate and assess requests on all matters relating to changes in the DNS root, including ccTLD delegations and redelegations. ICANN/IANA processes all requests for delegation and redelegation of ccTLDs, and encourages local Internet communities (including governments) to evolve broad-based, community-oriented policymaking and administrative structures. ICANN states that there are approximately 15 different categories of redelegation requests, each presenting or resulting from very different types of problems, challenges, and local situations. ICANN states that each request for delegation or redelegation is processed with sensitivity to its unique situation, following the policies documented in RFC 1591 and ICP-1, and in accordance with the ICANN Governmental Advisory Committee's Principles on Delegations and Redelegations.

Several papers suggested, or implied, that the functions of the Internet Assigned Names Authority (IANA) should be separated from the Internet Corporation for Assigned Names and Numbers (ICANN), or at least that the IANA functions should be provided to ccTLD operators even if the operator has not signed a contract with ICANN. It was stated that IANA funding should be separated from the funding of other ICANN activities and that top level domain name operators should oversee the IANA function. It was also stated that an assessment of ICANN's continuing management of the IANA function and whether it meets the needs of the global Internet community, should be made under an open and transparent renewal process, for the extension of the IANA contract after September 2003.

It was also suggested that there should be recognition of a nation's sovereignty over its ccTLD and the provision of an international framework within which nations can recognize other national ccTLDs and develop related policies in a multilateral environment. It was stated that ICANN should not attempt to impose binding policies on ccTLDs, since those policies are national matters.

One paper was suggested that the most fundamental issue that still remains to be addressed is that of internationalising the operation of the A root server system, because it does not appear to be desirable in public policy terms for most sovereign countries in the medium- to long- term that a single country should have total control of the World Root, since this could lead to the possible perception that the operation of the authoritative World Root may favour that country's own economic interests, unconsciously or otherwise.

Nominum presented a technical survey of ccTLD vulnerabilities and suggested several steps that would increase security and stability.

Verisign presented the model used for ".tv" (Tuvalu) and suggested that this experience had important lessons for how a public-private partnership in the DNS can contribute to economic growth and help close the digital divide.

It was suggested that any decisions to re-delegate a ccTLD should be made by the national government concerned in consultation with the Internet community of that country, and the existing and proposed ccTLD operator. An appropriate UN agency should determine the recognized national government of a country.

A paper by the Center for Democracy and Technology suggest that redelegation requests are more likely to succeed if the redelegation would be to a non-governmental, non-profit entity that broadly represents the national Internet community; if there is broad and documented support for the new entity; if there is a sound technical plan; if the principle of private sector self-regulation, with the government playing a supporting but non-intervening role is respected; if the new entity operates through open, transparent and inclusive processes; if the redelegation clearly benefits the local Internet community; if the government and the new entity agree to abide by ICANN's policies.

Syria stated that the ITU is the only suitable international organization to deal with Internet domain names and addresses and called for the workshop to lead to a series of steps towards the fulfillment of ITU's role in the domain, taking into considerations Resolution 102.

A group of African countries stated that it is imperative for ITU to undertake, from now on, a leadership role in the field of international cooperation towards the development and harmonization of policies in the key area of Internet domain names and addresses, and called on ICANN to fully cooperate with ITU in the implementation of Resolution 102 (Marrakesh, 2002) and on African regulators to implement a coordinated strategy for the defense of their interests regarding ICANN, in coordination with ITU.

AFNIC proposes to collaborate with ITU-D to expand its training and support activities for developing countries.

The International Chamber of Commerce (ICC) restated its support for ICANN as the appropriate organization to provide technical coordination of the Internet and policy matters directly related to it, matters which, states the ICC, are best driven by the private sector. ICC urges participants in the workshop to continue to work towards improving the stability and effectiveness of ICANN in the future.

ICANN's GNSO welcomes the interaction of ICANN with relevant governments and inter-governmental entities through the GAC, encourages governments and governmental entities to consider ICANN as the primary venue to address Internet naming and numbering issues within the mission of ICANN, and encourages and welcomes governments and governmental entities to attend and participate in ICANN's venues and meetings and to work actively within ICANN.

Dispute resolution rules and procedures for domain names are evolving and may go further than the Uniform Dispute Resolution Policy (UDRP). Also, it was suggested that improved methods to search for UDRP decisions could be useful.

There is increasing interest in Internationalized domain names (IDN) and a number of issues need to be discussed and agreed within specific language blocks.

It was suggested that increased cooperation between ICANN and intergovernmental treaty organizations (in particular ITU and WIPO) could be beneficial. In particular, ITU-T could help ICANN to achieve the ccTLD-government consensus that appears to be missing today.

Annex 1 contains a summary of the individual input documents.

## Annex 1

### Summaries of individual papers

This annex contains a summary of each individual input paper.

#### Doc 2: Norway

Domain names come under the provisions of the Telecommunication Act on the management of numbers, names and addresses for telecommunications networks and services. As a result they also fall within the jurisdiction of the Ministry of Transport and Communications and the Norwegian Post and Telecommunications Authority. However, these authorities have not yet exercised their authority to determine and assign domain names.

While the authorities have no direct powers over the Norwegian Service for Internet Domain Name Registration (NORID), at present, NORID is managed in “understanding with the Norwegian Post and Telecommunications Authority”, meaning that NORID has voluntarily agreed to parts of its operations being subject to the consent of the Authority. This relationship between NORID and the authorities functions extremely well.

However, one of the weaknesses of the existing system is primarily that the division of responsibility between NORID and the public authorities seems rather indistinct. This is largely because the division of responsibility is not defined within present regulations or agreements.

The Ministry has appointed a Working Group that was charged with the task of reviewing the management of the .no domain, the need for a body to resolve disputes over the rights to domain names, the withdrawal of assigned names, and appropriate measures for restricting domain piracy.

The Working Group is of the view that it is necessary to clarify the respective areas of responsibility of NORID and the public authorities. At the same time it should be stressed that the public authorities have a right and a duty to set guidelines for the management of .no. A certain degree of public control over the management of domain names is necessary if the authorities are to formulate a comprehensive policy on Information and Communication Technology (ICT) development. Furthermore a clearer framework for the assignment of names will facilitate greater predictability for holders of and applicants for domain names.

The Group considers that an overall objective must be that the country code top level domain .no should be the obvious choice for all Internet users resident in Norway. Furthermore, it is important that administration of the domain name should safeguard the interests of the users. The process of domain name assignment should for example be quick, of high quality and inexpensive.

In regard to the existing *administrative model*, the Group is of the view that the division of responsibility between NORID and public authorities needs clarification. The Group recommends that the .no domain should be managed in such a way that the Ministry of Transport and Communications and the Norwegian Post and Telecommunications Authority is given the overall political and administrative responsibility, with the right and duty to propose and be in charge of the legal framework for managing the .no domain. The Group recommends that the relationship between the authorities and the registration unit in Norway should be regulated in regulations prescribing the general framework and the specific conditions stating the management of the country code top level domain .no.

The Working Group has considered the existing *dispute resolution system* and has concluded that it should be extended to include third-party disputes. The Group recommends that a dispute resolution board should be established, based on NORID's existing dispute resolution committee (NOK), but

with an expanded authority to resolve third-party disputes. It is recommended that this system should be financed by a supplement to the registration fee and a fee payable by the complainant.

With regard to the possibility of *withdrawing unrightfully assigned domain names*, the Group recommends that the registration unit should be authorised to withdraw a domain name if it finds it obvious that an assignment is not in accordance with the assignment rules, Norwegian law, the rights of a third party, or if a domain name gives a wrong or incorrect impression that the holder is a public body.

### **Doc 3: Norway**

This paper presents the regulations developed in accordance with the principles outlined in Doc 2.

### **Doc 4: Peru**

The active participation of the government in ICT matters (and specifically in the Internet country code TLD ".pe") is based on the government's mandate to participate, together with the private sector, the academic sector, and the national Internet community, in the national technological development process. In particular, the government should act as facilitator of a process to develop an integrated policy for Internet domain names which is consensus-based and coordinated with all concerned national entities.

Indeed, the public interest related to the ccTLD .pe means that the government, which is the ultimate representative of the national public interests, should invite civil society and the private sectors, who are the fundamental drivers of national development, and the holders of domain names, to a national debate regarding the ccTLD .pe in order to come to an agreement on policies for this domain name.

The following general principles should apply:

1. The domain names corresponding to the ccTLD .pe are of public interest.
2. Private sector participation is essential as the driving force of development.
3. The participation of domain name holders is essential.
4. The participation of the government is essential to promote the Peruvian System of Domain Names (PSDN).

The PSDN ensures that the following are carried out:

1. Develop and maintain policies and regulations for the administration of the ccTLD .pe.
2. Integrate the representatives of the national Internet community.
3. Ensure that the administration of the ccTLD .pe takes place transparently, neutrally, and without discrimination.
4. Establish mechanisms to resolve disputes amongst domain name holders and with the ccTLD administrator.
5. Ensure that competition is free and fair.
6. Ensure compatibility at the international level.
7. Ensure that international standards are respected, and ensure stability and reliable operation.
8. Promote to citizens the use of domain names within .pe.
9. Coordinate the official representation of PSDN at the national and international levels.

## **Doc 5: WIPO**

WIPO has prepared "best practices" for the registration practices and the resolution of disputes related to the registration of domain names within ccTLDs.

Recognizing the wide variety in ccTLD registration conditions and procedures, the ccTLD Best Practices do not purport to be a tailor-made intellectual property protection scheme to be imported as such within a particular domain. Rather, they are to be viewed as a flexible framework built around a number of basic elements that are deemed critical from an intellectual property perspective. In this connection, it is clear that account will need to be taken of local legal and other requirements in the context of the implementation of the Best Practices in any particular ccTLD.

The ccTLD Best Practices constitute a set of minimum standards for the protection of intellectual property in the ccTLDs. While many additional protective measures are conceivable, the ccTLD Best Practices focus on those that are considered essential.

## **Doc 6: Michael Geist**

This paper reviews the relationship between **country code Top Level Domains (ccTLDs) and governments** in 45 countries. Included are 1) tables which highlight the main relationships,<sup>1</sup> and 2) country-specific information. The preliminary findings include:

1. Ten ccTLDs are government agencies or departments. In these cases the relationship is typically formalized between government and agency.
2. Nine ccTLDs are private, for-profit enterprises. Of these two (United States, Japan) have established a contractual relationship with the government, three have established an informal relationship, and four have no relationship with the government.
3. 20 ccTLDs are non-profit organizations. Four have formal, contractual relationships with their governments along with an ICANN agreement that governs their relationship. Five do not have a government relationship. Ten ccTLDs have informal relations with their government, of these, at least 3 are awaiting formalization of their relationship in the near future (Russia, South Africa, Italy).
4. Five ccTLDs are academic institutions; of these two have no relationship with their government. Two ccTLDs (Guatemala, Columbia) have battled takeover attempts by their government.
5. One ccTLD is managed by an individual. It is battling government attempts to take over the ccTLD management.

## **Doc 7: Vratislav Kurska**

Unique domain names, like brand names and trade marks, are intellectual property and registrars are not free, as they seem to believe, to cancel them at whim.

They can cancel registration, but not the ownership of intellectual property. Each registrar has the right to refuse or cancel the CONNECTION TO THE INTERNET of a particular domain name, but not the domain name itself. If the connection to the Internet is cancelled, the domain name owner should still retain ownership and should be free to seek connection of the "cancelled" domain name to the Internet through another registrar.

Therefore, there should be a global database of domain names independent of present registrars

---

<sup>1</sup> Appendix I provides an overview of the ccTLD-government relationships in tables.

### **Doc 8: Ethan Katsh**

This paper describes a scheme for publishing Uniform Dispute Resolution Policy (UDRP) decisions in such a way that searching for particular decisions is facilitated.

### **Doc 9: Spain**

The Spanish government has established the basic principles of the allocation system for domain names under the country code for Spain, namely *.es*.

The allocation criteria for *.es* domain names shall maintain the appropriate balance between, on the one hand, the confidence and legal certainty necessary for the development of electronic commerce and other electronic services and activities and, on the other, the flexibility and adaptability needed to respond to the demand for allocation of *.es* domain names, thereby assisting the development of the information society in Spain. Some of the key criteria are:

- a) The allocation of a domain name entitles the owner to use and to retain that name, provided the owner fulfils any particular requirements that may be established. In the event that the allocating authority finds evidence of a failure to fulfil such requirements, and on completion of the relevant procedures determined for each case, which shall include a hearing for the parties concerned, the domain name shall be cancelled.
- b) The owners of *.es* domain names shall comply with any technical rules and conditions which may be established by the allocating authority to ensure the smooth functioning of the *.es* domain name system.
- c) In accordance with applicable provisions, the allocating authority may establish an extrajudicial dispute resolution system concerning the use of domain names, including disputes over industrial property rights. This system shall provide the parties concerned with adequate legal guarantees, and shall not prejudice any legal action they may wish to take.

The corporate public entity *Red.es* is the allocating authority with responsibility for managing the register of *.es* Internet domain names.

### **Doc 10: Patrick O'Brien**

This paper suggests that the IANA function be separated from ICANN and in particular that the policy-development function be separate and independent of the operational (or secretariat) function.

### **Doc 11: Columbia**

The government of Columbia considers itself as having legal powers, under its telecommunications law, which defines telecommunications in very general terms, to intervene regarding the commercial exploitation of the ccTLD *.co*, in particular its re-delegation. It does not agree with the position taken by the University of Los Andes (the current operator of *.co*) that the domain *.co*, as a subject of Internet domain names, is a matter developed at an international private level, excluding Columbian legislation. In particular, it is noted that the ensemble of existing legislation applies to Internet actors, in particular laws concerning consumer protection and those vouching for the respect of the public.

The paper contains extensive descriptions of the historical developments of the Internet in general and the Domain Name System in particular, and explains the current situation in light of the evolution in the use of the Internet.

It argues that, under Columbian law, a ccTLD is not property that can be transferred. Instead, it is "of common use for all citizens" and, as such, no corporation or individual has a right to appropriate it.

It concludes that:

1. The domain .co assigned to Columbia as the country code in the Internet domain name system is of public interest.
2. The administration of the domain .co is intrinsically related to telecommunications. By such virtue, the national government is competent, through the Ministry of Communications, to put into action its planning, regulation and control without prejudice to the functions that may have been attributed to private operators.

### **Doc 12: Kim von Arx and Gregory Hagen**

This paper points out that, from a formal point of view, the US Department of Commerce (DoC) has control over ccTLD re-delegations, although, in practice, the DoC follows ICANN's recommendations. The paper argues that may give ICANN, in practice, a bargaining advantage with respect to the terms of contracts with ccTLDs.

The paper discusses the formation of ICANN and certain operational aspects of the Domain Name System and points out that, while the USA wished to exclude direct formal government intervention in Internet governance, it did not exclude its own interventions. The paper notes that the DoC re-delegated the ccTLD .us without intervention by ICANN and that there is no contract between ICANN and the .us operator.

It notes that the power of ICANN to threaten a ccTLD with potential redelegation or annihilation provides ICANN with a mechanism to ensure ccTLD compliance with ICANN policies and to force the adoption of ICANN-friendly contractual terms and conditions. These contractual terms and conditions can mandate or influence the types of policies that will be created and enforced by the ccTLD. Thus, to the extent that ccTLD policies impinge on domestic policy, they also diminish the sovereignty of nations to adopt laws independently of ICANN.

It concludes that in order to diminish the risks associated with foreign control over ccTLDs, countries need to gain control over their own ccTLD.

The paper argues that a political solution to the current issues would be to recognize a nation's sovereignty over its ccTLD and to provide an international regulatory framework within which nations can recognize other national ccTLDs and develop related policies in a multilateral environment.

### **Doc 13: Karl Auerbach**

This paper argues that the ICANN and IANA functions should be separate and that ccTLDs should be able to obtain IANA services even if they have not signed a contract with ICANN.

The paper expresses a concern that ICANN may be withholding IANA services in order to induce ccTLDs to enter into contracts with ICANN.

### **Doc 14: Columbia**

These are the regulations adopted in Columbia with respect to the administration of the domain name .co.



The "considerings" affirm that the domain name .co is of public interest in the telecommunications sector, and that, therefore, the government has powers which it will exercise through the Ministry of Communications. They refer to the consultation presented in Doc 11 and to ITU Resolution 102.

The regulations contain a number of "resolves", including the following:

1. The Internet domain name .co is matter of concern to the telecommunications sector, of public interest, whose administration, maintenance and development is subject to the planning, regulation, and control of the government, through the Ministry of Communications, in order to favor global telecommunications and their provision for the users in Columbia.

### **Doc 15: Scott Donahey**

This paper presents the dispute resolution procedures adopted for .cn. The provisions adopted differ from the Uniform Dispute Resolution Policy (UDRP) in significant and far-reaching ways. Certain powers under the CNNIC DRP are reserved to CNNIC, granted to the providers, or reserved for the panel which were either not contemplated under the UDRP or were assigned in a completely different manner by the UDRP. In addition the parties' rights under the CNNIC DRP are decidedly different from those granted under the UDRP. Finally, the elements which a complainant must establish in order to prevail under the CNNIC DRP are significantly different from those under the UDRP.

While it is unclear how the specific provisions will be interpreted and applied by the panels ultimately charged with deciding cases under the CNNIC, there are surely dramatic differences from the UDRP, and there are potential differences even more dramatic and far reaching, depending on the interpretation and application by the panels and any interpretation by CNNIC. At the least it should be noted that the CNNIC DRP intends to extend its application to personal and organizational names, as well as marks. Second, protection in marks applies more broadly than simply to registered marks, and perhaps even more broadly than to common law marks, depending on what is meant by "civil rights" or "interests" in a mark. Third, criticism sites, generally given protection under the UDRP, appear to be illegitimate under the CNNIC DRP. Finally, the degree to which the panelists will be asked to consider and apply the provisions of the CNNIC Domain Name Rules is not absolutely clear.

### **Doc 16: Guinea Bissau**

Because of new legal view in the country and worried about constant growth numbers of users "Local Internet Community"; considering the vital importance of this service in the globalisation context, having on the other hand consideration that ccTLD is a strategic resource and of public interest, therefore it is attached to national sovereignty, the Government expressed its intention to redeem the ccTLD gw with objective of adapt its new Global management.

Since privatisation and the creation of the independent regulatory agency (ICGB) in 1999, it is collecting information about redeem process management of ccTLD unfortunately there was not success.

### **Doc 17: Guinea Bissau**

This is the basic telecommunications law, which defines telecommunications in very general terms (but excludes broadcasting). Its goals are:

1. Promote the development of telecommunications in Guinea-Bissau through the definition of an adequate legal framework in accordance with globalization demands;

2. Promote and emphasize the role of telecommunications as a fundamental instrument in economic and social development;
3. Create conditions favorable to the emergence and development of competition in the telecommunications sector in order to facilitate access to users of new services at the best prices;
4. Develop and improve telecommunications services of public use aiming at a better coverage nationwide in terms of universal access to telecommunications;

### **Doc 18: Guinea Bissau**

This is a policy statement. It includes the following statements.

The telecommunications sector has entered a spectacular era of change and growth at all levels. In fact, telecommunications began to play a central role in the interaction process between various sectors of the economy. This revolution was given impetus by the great technological development and the globalization of the economy as well as the exploration of telecommunications services.

Thus, the liberalization and privatization of public enterprises carried out in developed countries allowed the creation of consortia that grouped together suppliers worldwide aiming at the exploration of new services. By and large these services had their purpose to meet specific needs felt by companies and private individuals.

Globalization of capital movements fostered merger or joint participation beyond borders between enterprises involved in telecommunications, as well as alliances that take on increasingly a multilateral and worldwide dimension.

This explosion of changes has spread to all every developing country, and within ECOWAS in particular, results obtained are satisfactory in countries that have already begun restructuring the sector, namely Ghana, Cote d'Ivoire and Senegal.

Guinea-Bissau could not stand aloof from these rapid changes, and the current Declaration of Sector Policy shows to which extent the telecommunications sector is a focus of government's most pressing concerns.

Telecommunications are a strategic sector in any country. They are a central element of economic activities and constitute an essential instrument for the implementation of policies designed to integrate the rural world, besides being a sector particularly sensitive to democratic transition and State defense and security.

Guinea-Bissau opts clearly for liberalization of the telecommunications sector. This political option is expressed by government's wish to define a legal framework adapted to new realities within this sector at the regional and world levels.

### **Doc 19: Nominet**

Nominet does not recognize ICANN or its various actual and putative supporting organizations as an appropriate or legitimate vehicle for determining Nominet's own policy, or indeed the policy of any other ccTLD manager. Specifically the remit of an advisory organization to ICANN should be limited to advising ICANN on ICANN's own policy toward ccTLD managers. If ccTLD managers require their own policy advice, they should obtain it elsewhere as they see fit. Nominet distinguishes this from the sharing of best practice between ccTLD managers, which, as stated below, it considers important, and Nominet accepts that ICANN might have a useful role to play in this respect.

Each ccTLD manager needs to develop its own policies according to local laws, customs, and regulatory and business environment, as well as the demand for registrations.

ICANN, as the current IANA operator, should bear in mind that IANA's function with respect to ccTLDs should be to record the details of the name-servers within the root zone file, to change these on the instruction of the designated ccTLD manager, and to publish the root zone file to root server operators. In respect of ccTLDs, there is no requirement on ICANN to exceed these simple IANA functions.

Any decisions to re-delegate a ccTLD should be made by the national government concerned in consultation with the Internet community of that country, and the existing and proposed ccTLD operator, and neither by ICANN, IANA, nor by vote of other ccTLD operators. An appropriate UN agency should determine the recognized national government of a country.

### **Doc 20: Nominet**

Nominet does not believe that the ccNSO, or ICANN, should develop policy which is binding on ccTLDs - "binding" implies some means of enforcement or penalty if the ccTLD fails to comply - a power not appropriate for ICANN to wield against the national interests of a ccTLD and its Local Internet Community, this latter being the appropriate mechanism to define ccTLD policies and ensure that they are complied with (in particular for what concerns data privacy, consumer protection, competition, etc.).

### **Doc 21: Saudi Arabia Network Information Center**

King Abdulaziz City for Science and Technology (KACST) is an independent scientific organization administratively belonging to the Prime Minister. Moreover, KACST has played a fundamental and positive role also in the introduction of the Internet to the Kingdom of Saudi Arabia in the end of 1998 based on a Royal decree in which an Internet Services Unit (ISU) was established. SaudiNIC is a subdivision of KACST's ISU and it is the entity that is responsible for the administration of the domain name space for the country code (ccTLD) of Saudi Arabia (.SA). This includes the operation of the DNS root servers for .SA domains as well as the registration and maintenance of all third-level .SA domain names. Additionally, SaudiNIC is a Local Internet Registry (LIR) authorized by RIPE-NCC, which is responsible for allocating blocks of IP addresses to universities and local ISPs in Saudi Arabia.

The mission of SaudiNIC is to provide an equitable, just and competent technical and administrative management of domain name registrations and IP address allocations for Internet community in Saudi Arabia.

The paper contains a very clear and complete description of SaudiNIC's policies and operations.

Since the Internet was originally evolved in the United States, it supported only 7-bit ASCII code (English characters), and the Domain Name System (DNS) supports alphabets, numbers and hyphen of the ASCII code. The activity of supporting multilingual characters in domain names is becoming very important now along other Internet internationalization to make the Internet globally accessible and become ubiquitous. Therefore, using the Arabic language to express Internet domain names is becoming also important and a number of solutions and implementations have been introduced in the market but based on non-open standards. Also, there is some non-for-profit international organizations that are trying to promote the multilingual issues and standards on the Internet, such as MINC (Multilingual Internet Names Consortium) and AINC (Arabic Internet Names Consortium).

One of the strategic tasks of AINC is to setup some linguistic guidelines to be used by technology providers. Therefore, an Arabic Linguistic Committee was established during the formation of

AINC in April 2000 to carry this task. The main goals of the committee are (a) to define the accepted Arabic character set to be used for writing domain names in Arabic, and (b) to define the top-level domains of the Arabic domain name tree structure (i.e., Arabic gTLDs, and Arabic ccTLDs).

## **Doc 22: Spain**

Given the increasing expansion of Internet in Spain, and its use in the commercial arena, the domain name ".es" has acquired great importance as a tool for the development of the Information Society in Spain and as an instrument for the implementation of government policies in this area.

The management of ".es" by a public entity and the implementation within the framework of regulations defined by the government make ".es" a special domain name. This paper covers the following areas:

- Evolution of ".es" management and its main characteristics
- How domain names are assigned under ".es"
- Costs of domain names under ".es"
- Relations with the local internet community

By the law 14/2000 of 14 December 2002, the designation of Retevision, a public entity supervised by the Ministry of Development, as manager of ".es", was formalized. The main points flowing from this law and related regulations and decrees are summarized in the summary of Doc 9.

## **Doc 23: Switzerland and Switch**

The Internet has grown to become in a few years an essential element of the economy, in particular for the development of electronic commerce and the information society. Therefore domain names have acquired a fundamental importance. This is the main reason why the Swiss government has considered it necessary to formalize legally the registration of domain names under the ccTLD ".ch". To do this it issued rules (regulations) that are contained in the decree on Addressing Resources in Telecommunications (ORAT). This decree entered into force on 1 April 2002.

The ccTLD operator is Switch, a non-profit foundation whose mission is to operate the Swiss academic network. Switch participated in the development and implementation of Internet from its early days.

The government entity responsible for the regulations related to domain names is the Federal Office of Communications (OFCOM), which regulates all forms of telecommunications, including fixed telephony, wireless telephony, and broadcasting.

On the basis of a national consultation, OFCOM determined that there was no support for introducing a competitive registry-registrar model in Switzerland, and that there was no reason not to continue with the single-provider model implemented by Switch. However, OFCOM could revisit this topic if market conditions change.

The key point of the Swiss situation are:

- Internet domain names and addresses are subject to regulation by OFCOM just like any other telecommunications resource
- OFCOM designates the ccTLD operator. It can do this by setting conditions or by calling for public tender. OFCOM establishes a 5-year (renewable) public law contract with the ccTLD operator.

- A dispute resolution procedure for domain name should be put in place.
- General rules of allocation for telecommunications resources must be respected by the ccTLD operator, in particular transparency and non-discrimination.
- Prices are set freely by the ccTLD operator are supervised and approved by OFCOM on the basis of costs and fair profit margins.
- Any contracts between SWITCH and ICANN would have to be approved by OFCOM.

#### **Doc 24: ICANN**

ICANN has a well-defined mission: to coordinate the administration of the Internet's systems of unique identifiers (domain names, Internet protocol addresses, and protocol port and parameters numbers). In this context, ICANN also develops global policies as reasonably necessary to its main technical mission. In simplest form, ICANN's core mission is the stability of the Internet's naming and addressing systems.

To accomplish its mission, ICANN fosters collaborative relationships with Internet stakeholders worldwide, including governments, infrastructure providers (such as country-code top-level domain (ccTLD) registries, generic top-level domain (gTLD) registries and registrars, IP address registries), Internet service and connectivity providers, the community of technical experts and architects, the private sector, business and non-commercial users, and a wide range of advocates, interest groups, and associations.. ICANN is a global public/private partnership dedicated to operating in an open and transparent manner. There are no membership fees and anyone can participate in its work. In essence, ICANN is an open forum for building consensus.

ICANN operates according to a Memorandum of Understanding with the U.S. Department of Commerce. Under the MOU, ICANN handles matters relating to the domain name system's top-level domains, including any changes to be made to the DNS Root Zone File, subject to the final approval of the DoC. Under this agreed framework, a request for delegation, redelegation, authoritative name server changes, and so forth, are submitted to and processed by ICANN. ICANN is not a government or a regulator, but acts as an experienced, neutral, expert gatekeeper for the DNS root zone file, working closely with local Internet communities (including governments) to nurture responsive, accountable operation of country-code top-level domain registries.

#### **Doc 25: ICANN**

Any organization, whether new or well established, benefits from periodic 'self assessments' of what and how it can improve. In 2002, ICANN completed a community-based self-evaluation, that resulted in a series of significant reforms. This paper focuses on the status and effect of these reforms with respect to ccTLDs and governments.

Under the reformed structure, there will be a Country Code Names Supporting Organization (ccNSO) directed to matters of global policy and other issues affecting ccTLDs. Work towards the structure of this supporting organization is nearing completion, and will be finalized by the next ICANN Board meeting in late March 2003.

ICANN is a public/private partnership in which governments play a critical role. Governments and distinct economies participate in ICANN through the Governmental Advisory Committee (GAC). Governments representing over 90 percent of the world's Internet users participate actively in the GAC; membership is open to all national governments and distinct economies; and, on invitation of the GAC through its Chair, other governmental and international treaty organizations.

The GAC played an important role in the ICANN reform discussion, advising on structures and processes to strengthen governmental participation in ICANN and to integrate governmental advice more firmly into the ICANN decision process where matters of public policy are involved. The GAC plays a key part in issues affecting ccTLDs and their relationships with their governments.

### **Doc 26: ICANN**

Country-Code Top-Level Domains, or ccTLDs, were initially delegated by Dr. Jon Postel (the remarkable Internet architect originally entrusted with responsibility for deployment of the Internet's domain name system) with the objective of enabling local Internet communities worldwide to develop their own locally-responsive and -accountable DNS services, and to encourage all parts of the world to 'get online'. Initially, from the mid-1980s to the mid-1990s, ccTLD registry responsibilities were typically delegated to Internet pioneers, often from the academic or research communities. In 1994, Dr. Postel published the basic policy and technical requirements for TLD delegations, redelegations, and operations in a document known as RFC 1591.

Today, in a vastly more complex global Internet environment, ICANN carries on Dr. Postel's work by seeking to institutionalize and document the framework for ccTLD delegations, consistent with the existing published policies. In this role (known as the IANA function"), ICANN has the responsibility to investigate and assess requests on all matters relating to changes in the DNS root, including ccTLD delegations and redelegations. ICANN/IANA processes all requests for delegation and redelegation of ccTLDs, and encourages local Internet communities (including governments) to evolve broad-based, community-oriented policymaking and administrative structures. These frameworks of accountability help to advance stability and clarify responsibilities both at the local community level and for the overall global Internet.

There are approximately 15 different categories of redelegation requests, each presenting or resulting from very different types of problems, challenges, and local situations. Additionally, there are numerous ccTLD management models, often reflective of the national situation. Every country and territory is obviously unique, with its own particular institutions, populations, interests, history, connectivity, stakeholder interests, form of government, public policy objectives, and so forth. Accordingly, the exact contours of each such framework of accountability will vary in certain respects, subject to the fundamental global policies designed to ensure global interoperability and operational stability of the Internet's DNS. Each request for delegation or redelegation is processed by ICANN with sensitivity to its unique situation, following the policies documented in RFC 1591 and ICP-1, and in accordance with the ICANN Governmental Advisory Committee's Principles on Delegations and Redelegations.

### **Doc 27: TSB**

In the context of the Workshop, an invitation E-Mail was sent to each of the ccTLD operators listed on the IANA web site at <http://www.iana.org/cctld/cctld-whois.htm>, from 3 to 6 December 2002. In certain cases, the E-Mail address was apparently not valid, since an "undeliverable" message was returned to us. The paper contains the list of delivery failures. The information contained in the paper was provided to IANA in January 2003.

### **Doc 28: Nominet**

With respect to the US Department of Commerce's (DoC) proposal to renew on a sole-source basis the IANA contract with ICANN, Nominet states that it fully supports DoC's goal to ensure the stability and future expansion of the Internet, but expresses some concerns with the proposed renewal. Nominet believes that some consideration should have been given to consulting more

widely with ccTLD operators and that an open call for tenders might have been more appropriate. Nominet states that the IANA function should meet the following requirements:

1. Respect policies developed nationally outside the USA.
2. IANA funding must be clearly separated from the funding of any associated policy-making role or any oversight role of gTLD registries and registrars.
3. The IANA function should be funded and overseen by the Top Level Domain operators themselves.
4. The IANA function should be carried out in a not-for-profit regime.

### **Doc 29: Liz Williams**

This paper sets out the development of Internet governance in Australia. It describes the history of the administration of the .au country code, the formation of a private sector not-for-profit regulatory structure and provides some commentary on particular aspects of the establishment of new models for managing the technical resources of the global Domain Name System (DNS).

### **Doc 30: TSB**

The ITU-T is one of the operating sectors of the ITU. Its primary mission is to develop non-binding standards (called Recommendations) covering all fields of telecommunications and to act as registration authority for certain numbering resources, for example international country codes for telephone numbers, Subscriber Identification Module (SIM) numbers used in GSM mobile phones, Signaling Area Network Codes (SANC), etc.

ITU-T's membership consists of 189 governments and about 500 industry members. ITU-T's main role is to provide a forum for discussion, coordination, and consensus-building between its members, including governments and industry.

The ITU-T performs world-wide administration, and acts as the forum for policy management, of a number of naming and address allocation systems that are essential for the good functioning of critical infrastructures, including the physical-layer infrastructure of the Internet itself. We cite here only such well-known examples as the E.164 numbering resource and the E.212 mobile numbering resource.

The presence in ITU-T of developing country governments broadens participation to people in those countries who would not otherwise have been represented. Thanks to the maturity of the processes and procedures, there are sufficient checks and balances in place to ensure that vested interests cannot misuse ITU processes for their particular interests.

Both government and industry membership of ITU-T, and both government and industry participation in ITU-T technical and governing bodies, are allowed under the existing ITU Constitution and Convention, and have been in place for many years, with satisfactory results.

As IP-based networks and IP-based services have become more and more widely used to provide services similar to those of traditional telecommunications networks, ITU-T has increased its involvement with the new technologies. It should not be forgotten that the physical infrastructure which is required for Internet is based on ITU-T Recommendations, ranging from modem specifications such as Recommendation V.34 to Recommendation X.509 which provides the basis for public key infrastructure (PKI).

ITU-T is an effective public-private partnership, rooted in the public sector but with the active backing and participation of industry players. In the ITU-T industry and governments work

together, to achieve common goals for the public benefit. And ITU is unique in being a partnership between governments and industry for information and communication technologies (ICT).

It is widely acknowledged that the ITU-T performs its tasks to the general satisfaction of industry, governments, and the public at large, using processes that are open, transparent, and ensure accountability to all stakeholders.

There is a misperception that if an issue is coordinated within ITU, it will be "controlled" by the ITU or by governments. This is not correct. Government participation and coordination do not amount to government control. A good example is the international telephone numbering scheme, which is coordinated by ITU-T and is universally considered to work to the satisfaction of the general public; however, telephone services are not controlled by ITU-T.

Thus it appears that ITU could increase its cooperation with ICANN, to mutual benefit. The modalities of such increased cooperation remain to be discussed and agreed. In accordance with the instructions contained in ITU Resolution 102 (Marrakesh, 2002), ITU-T will also work with Member States with respect to their experiences with ccTLDs and would invite ccTLDs to participate in this process to address issues of common interests.

### **Doc 31: TSB**

This is a presentation, which makes, among others, the following points:

ITU-T does not do the following:

1. World-wide regulation
2. Consider issues that are national matters
3. Binding recommendations
4. Top-down decisions
5. Impose contractual terms or operating rules on private companies
6. Work in non-transparent ways
7. Act bureaucratically
8. Have staff that decides policies
9. Collect fees other than membership fees (with the exception of minor cost-recovery activities)

The presentation gives a summary of certain issues that have been raised by ccTLD operators, for example:

1. ccTLD policies are national matters
2. The IANA function should be carried out by a trusted international body
3. Re-delegations should be handled locally, in accordance with national laws and regulations
4. Regulation should be done by governments

The presentation includes questions raised by ccTLDs with respect to ITU and answers to those questions.

It concludes that, since ITU-T is a successful government-industry partnership, with fast and effective working methods, ITU-T could help ICANN to achieve the ccTLD-government consensus that seems to be missing today



### **Doc 32: Japan and JPRS**

On 5 August 1986, the .jp top-level domain was delegated to Jun Murai by the Information Sciences Institute, University of Southern California, which then performed the functions of the Internet Assigned Numbers Authority (the IANA). After an initial period of more informal management, in December 1991 the Japan Network Information Center (JNIC) was founded to provide a framework for operation of the .jp top-level domain. In April 1993, with Jun Murai's consent, JNIC reorganized itself as JaPan Network Information Center (JPNIC), with ISPs, research networks, and academic networks located in Japan as its members. On 31 March 1997, JPNIC obtained approval from the Science and Technology Agency, the Ministry of Education, Science, Sports and Culture (these two organisations are now merged into the Ministry of Education, Culture, Sports, Science and Technology), the Ministry of International Trade and Industry (currently the Ministry of Economy, Trade and Industry), and the Ministry of Posts and Telecommunications (currently the Ministry of Public Management, Home Affairs, Posts and Telecommunications) to operate as a corporate body.

The ccTLD operator, which formerly was JPNIC, is currently Japan Registry Service Co., Ltd. (JPRS) as from 1 April 2002. Likewise, administrative contact was Jun Murai and is now Koki Higashida, President and CEO of JPRS.

The remainder of the paper provides details on the re-delegation process and JPRS operating and dispute resolution procedures.

### **Doc 33: CNNIC**

This is a presentation, which covers the following areas:

- Administrative Pattern
- Structure
- Policies and Regulations
- Evolution of .CN Domain Names
- Reform of .CN Domain Names
- Formulate the regulations and policies concerning the administration of the Internet domain names; Establish the system for Country (or Regional) Code Top Level Domain (ccTLD) under .CN and Chinese domain names; Administer the registry of .CN ccTLD and Chinese domain names; Supervise and administer the domain name registration service; Be in charge of the international coordination regarding domain name issues. CNNIC is responsible to
- Operate, maintain and administer the corresponding top-level domain name servers and databases, ensure the secure and reliable operation of DNS;
- Formulate rules concerning the domain name registration in accordance with the Regulations;
- Select domain name registrars based on the principle of non-discrimination;
- Supervise and administer the registration service provided by domain name registrars; Appoint the third party as neutral domain name dispute resolution institution;
- Other duties designated by the MII

The remainder of the presentation provides details on CNNIC operations and policies.

### Doc 34: France

In France, the arrangements for the management of ".fr" were defined having regard to certain principles:

- the DNS is a public resource which must be managed in the general interest;
- the ccTLD manager must have the support of the local Internet community and of the Government or competent public authorities;
- the name space must be a space that Internet users can trust.

In this spirit, the *Association Française pour le Nommage Internet en Coopération* (French Network Information Center) (AFNIC) was set up in December 1997 on the joint initiative of INRIA and the State, the latter being represented by the Ministries responsible for telecommunications, industry and research. A not-for-profit association governed by the French Act of 1 July 1901, AFNIC brings together all Internet players: users, providers and public authorities.

The rules for the management of ".fr" are defined by AFNIC, whose decisions are binding on all ".fr" users.

The fact that the ".fr" management rules were initially very restrictive had the effect of dissuading "cyberpiracy" and of limiting conflicts to just a few cases per year; at the same time however, it limited the number of ".fr" registrations. In consultation with all the players concerned, AFNIC gradually relaxed the ".fr" management rules while maintaining the principle of an *a priori* control over registrations.

The vast majority of domains are registered by companies asserting an intellectual property right (business name, brand, etc.) over the name requested. AFNIC performs the necessary checks by consulting the details of such companies in the relevant official online databases (trade or brand register).

AFNIC's current management of ".fr" appears rigorous enough to avoid conflicts and to make for Internet user confidence by ensuring proper identification of domain name holders and requiring proof of an intellectual property right over the names being registered. It has become sufficiently flexible to make ".fr" more attractive to users.

Consultations organized at the request of the Government served to confirm that the majority of users were satisfied with the balance achieved in the management of ".fr", which will nevertheless need to continue evolving in order to take account of new user requirements and of changes in the international DNS management context.

The top-level domains (ccTLDs) corresponding to the French overseas *départements* and territories were delegated by IANA to various operators without the French authorities having been consulted at the time.

a) In addition to ".fr", AFNIC manages ".re" (Réunion), ".pm" (St Pierre and Miquelon), ".yt" (Mayotte) and ".wf" (Wallis and Futuna). All of the domains other than ".fr" were frozen (no registration possible) until 2001.

At the request of the Government, and following consultation of the local players and ministries concerned, particularly with a view to drawing up an appropriately tailored *charte de gestion*, AFNIC opened the doors to registration under ".re" in June 2001, with 170 domains having been registered as at January 2003.

b) The codes ".pf" for Polynesia and ".nc" for New Caledonia are open and are managed by public entities, namely the *Office des Postes et Télécommunications* (OPT) and the *Institut de Recherche pour le Développement* for ".nc". Within these territories, competence in the field of

telecommunications falls to the territorial authorities and not to the Minister responsible for telecommunications.

c) The other domains are managed by private companies.

The legal basis for the French approach is given in a law: Article L. 34-11 of the *Code des Postes et Télécommunications*:

"Art. L. 34-11. - I. - The Minister responsible for telecommunications shall, following public consultation, designate the entities responsible for allocating the domain names, within the top-level domains of the Internet domain names addressing system, corresponding to the national territory. The performance of their duties shall not confer upon the entities thus designated any intellectual property rights over the domain names.

Domain names shall be allocated by the aforementioned entities in the general interest, in accordance with rules that are non-discriminatory and publicly available and which respect intellectual property rights.

In the event that the entities should cease their activities, the State shall have the right of use of the domain name database they previously managed.

The Minister responsible for telecommunications shall see to it that the entities duly respect the principles set forth in the second paragraph. He may decide to withdraw the designation of an entity, after having given the latter an opportunity to present its remarks, in the event that it is found to be ignorant of the provisions of the present Article. Each entity shall submit to the Minister an annual report.

A State Council decree shall, as necessary, specify the conditions governing application of the present Article.

II. - Without prejudice to their application by right on Mayotte pursuant to Article 3.I.8 of Act No. 2001-616 of 11 July 2001, the provisions of I shall be applicable in Wallis and Futuna and in the French Southern and Antarctic Lands.

The entities responsible for allocating domain names in New Caledonia and in French Polynesia shall not hold any intellectual property rights over those names."

### **Doc 35: KENIC**

The administration and technical operations of the Kenyan Country Code Top Level (ccTLD) Domain, like many other Country Code Top Level domains, was initially under the 'Internet Pioneer', Jon Postel. In April 1993, the Internet Assigned Numbers Authority (IANA) delegated the administration of the .ke registry to Dr. Shem J. Ochuodho, Kenya, while Mr. Randy Bush, United States, took up the Technical Contact, providing technical and domain name registration for the .ke registry on voluntary basis.

In May 2000, a group of Kenyan Internet stakeholders and the Kenyan Government launched an initiative to form a participatory, community-based non-profit organization located in Kenya to manage both the administrative and technical aspects of the .ke ccTLD registry. The Kenyan Internet stakeholders included the Communications Commission of Kenya (CCK), the Government Directorate of Information Technology Services, Computer Society of Kenya (CSK), Kenya Education Network (KENET), Kenya Information Society (KIS), Nationwide Taskforce on Electronic Commerce (NTFecom), the Telecommunications Service Providers Association of Kenya (TESPOK), the East African Internet Association (EAIA) and the Network Operators Association (Telkom Kenya).

While the Kenyan Internet community and the Government appreciated the good work done by both the .ke ccTLD administrative contact Dr. Shem Ochuodho and the technical contact Mr. Randy Bush, they strongly felt that the task at hand had increasingly become too great for one person and a better suited organization which was representative of the local Internet community needed to be established with the appropriate resources to move Kenya forward in the global world of the Internet with the full support of the Government.

Through the Internet stakeholders and the Government initiative, there have been broad-based consultations and research facilitated by the Communications Commission of Kenya (CCK), since October 2001, to achieve these objectives.

As a result of several meetings held and wide range consultations, the Kenya Network Information Center, KENIC, was born and registered under the Kenyan laws as a company limited by guarantee (a not-for-profit entity) to manage the administration and technical operations of the Kenyan ccTLD. In addition to performing the technical, administrative, and policy-setting functions for the .ke registry, a stated objective of KENIC is to "promote, manage and operate the delegated .ke ccTLD in the interest of the Kenyan Internet community and being mindful of the global Internet community interest in consistent with Internet Corporation for Assigned Numbers and Names (ICANN) policies."

The remainder of the paper gives details on the re-delegation process.

### **Doc 36: ICANN GAC**

In the five years since the issuance of RFC 1591, the Internet has evolved from a tool reserved for computer and networking research, to a global medium for commerce, education, and communication. The new realities of the Internet, including its increased importance as a vehicle for national economic growth, and the expanding and more diverse nature of the Internet community necessitated evolution in the traditional means of managing and administering Internet technical functions.

As a result, DNS functions, including the administration of the DNS root server system, the development of policies for the registration and allocation of domain names, the coordination of Internet Protocols, and the delegation of Internet Protocol numbers are becoming more clearly delineated and formalised through the ICANN process. Similarly, the procedures and framework of accountability for delegation and administration of ccTLDs need to evolve into a more robust, certain, and reliable system as well.

While evolution is needed, the principle of RFC 1591 remains sound: the manager of a ccTLD performs a public service on behalf of the relevant local community and as such the designated manager has a duty to serve this community. The designated manager also has a responsibility to the global Internet community. By 'global Internet community' we do not mean any specific legal or international entity, but rather we interpret the term to refer to all of those who are affected by, now or in the future, the operation of the relevant TLD, because such operation may impinge on more than one jurisdiction and affect the interests of individuals and entities from both within the relevant country or territory and elsewhere. This is our interpretation of the meaning of 'global Internet community' as it is used in RFC 1591.

The objective of this document is to suggest principles that will assist in the development of best practice for the delegation and administration of ccTLDs. These principles are intended to contribute to the development of models of:

- a communication between the relevant government or public authority and ICANN;
- a communication between ICANN and the delegee; and

- a communication between the relevant government or public authority and the delegee.

The remainder of the document provides the actual principles. For example:

- The relevant government or public authority ultimately represents the interests of the people of the country or territory for which the ccTLD has been delegated.
- Governments or public authorities have responsibility for public policy objectives such as: transparency and non-discriminatory practices; greater choice, lower prices and better services for all categories of users; respect for personal privacy; and consumer protection issues. Considering their responsibility to protect these interests, governments or public authorities maintain ultimate policy authority over their respective ccTLDs and should ensure that they are operated in conformity with domestic public policy objectives, laws and regulations, and international law and applicable international conventions.

It also provides guidelines for communications between the ccTLD operator, ICANN and the national government.

### **Doc 37: USA**

In 1992, the National Science Foundation (NSF) entered into a cooperative agreement with Network Solutions Inc. (NSI) to provide registry and registrar services for generic top level domains, including the .com, .net, .org, .gov, and .edu domains, as well as the .us domain. In 1993, NSI provided funding to the University of Southern California's Information Sciences Institute (USC/ISI) to serve as the .us registrar. USC/ISI continued in this role through September 2000.

Dr. Jonathan B. Postel of USC/ISI originally administered the .us domain as a locality based hierarchy in which second-level domain space was allocated to states, U.S. territories and special purposes as described in the Internet Engineering Task Force's (IETF) RFC 1480. The .us domain was further subdivided into localities and other functional designations and became a widely distributed registry with over 11,000 domain delegations to over 800 individuals and entities. These delegated managers maintained a registry and provided registration services for commercial, educational, and governmental entities in the space. Under this system, the .us domain was generally used by U.S. state and local governments, although some commercial names were assigned. Where registration for a locality had not been delegated, Dr. Postel served as the registrar.

#### *The Department of Commerce's Role in the Development of Policy for the .us domain*

On July 1, 1997, as part of the *Framework for Global Electronic Commerce*, the President directed the Secretary of Commerce to privatize management of certain technical aspects of the Internet domain name system (DNS) in a manner that would increase competition and facilitate international participation in DNS management. In response to this directive, the Department of Commerce, through the National Telecommunications and Information Administration (NTIA), began a process of gathering public comments to develop the U.S. Government's policy regarding privatization of certain technical aspects of the DNS, including a commitment to further explore and seek public comment about the evolution of the .us domain. In September 1998, NSF transferred its cooperative agreement with NSI to the Department to permit a ramp down of the agreement as part of the privatization process.

In a policy development process paralleling the Department's privatization efforts, NTIA began an extensive outreach effort to the U.S. Internet stakeholder community on the expansion and future administration of the .us domain, including an initial request for public comment in August 1998. Early the next year, NTIA hosted a public meeting regarding the future management and administration of the .us domain with approximately 60 participants, including the then-current

usTLD Administrator; then-current .us registrars; educators; representatives of the technical, public interest, and business communities; and federal, state and foreign government officials. Afterwards, NTIA established an open electronic mailing list to facilitate further public discussions of the issues.

Through this public outreach process, NTIA learned that the distributed registration model developed for the .us domain afforded scalable registration services and opportunities for commercial entities to provide name registration services. However, because of the relative lack of public awareness about the availability of .us domain domain names and its deeply hierarchical and somewhat cumbersome structure, the .us domain had not attracted a high level of domain name registration activity and remained under-populated in comparison with other ccTLDs. Some commenters suggested that the general absence of non-locality based registration space in the .us domain contributed to the perceived overcrowding in the generic .com, .net, and .org top level domains. There was general consensus in the U.S. Internet stakeholder community that opening the .us domain to direct second-level domain registrations would increase the attractiveness of the space to most consumers.

In an effort to develop a more concrete framework for obtaining new services for the .us domain identified during the public comment process, NTIA prepared a draft Statement of Work to be incorporated in a request for proposal for management and administration of the .us domain. This draft Statement of Work was also subject to public comment and amended accordingly. The Department then began a competitive procurement process, which resulted in the award of a contract to NeuStar, Inc. (NeuStar) for the provision of administrative and technical services for the .us domain.

The Department awarded NeuStar a four-year contract (with two one-year, optional extensions) that sets forth the terms for the technical management of .us and a number of enhanced services for .us consumers. In the contract, the Department of Commerce outlines the U.S. Government's objectives for the .us domain:

- To ensure that the procedures and a framework of accountability for the delegation and the administration of the .us domain evolve into a more robust, certain, and reliable system.
- To promote increased use of the .us domain by the U.S. Internet community, (including small businesses, consumers, Internet users, not-for-profit organizations, and local governments (i.e., state, city, and county), among others, with residence or a bona fide presence in the United States through introduction of enhanced services, dissemination of information through advertising and/or other appropriate mechanisms, and simplification of registration services including direct registration.
- To create a centrally administered and efficiently managed structure that ensures both registrant/consumer confidence and infrastructure stability through coordination of delegations as well as other appropriate functions.
- To create a stable, flexible, and balanced environment within the .us domain that is conducive to innovation and that will meet the future demands of potential registrants.
- To ensure continued stability of the domain name systems as a whole and the .us domain, particularly throughout the transition period from the current management structure into the new structure developed and maintained under the contract.
- To manage the .us domain consistent with the Internet Corporation for Assigned Names and Numbers' (ICANN) technical management of the DNS.
- To allow for the adequate protection of intellectual property in the .us domain.

- To establish and maintain consistent communication between the Department, the Contractor and ICANN. This includes representation of the .us domain in the ICANN ccTLD constituency and contribution to ICANN's operating costs as apportioned to the .us domain through the ICANN budget process.
- To promote robust competition within the .us domain and in particular registration services that will lead to greater choice, innovation, and better services for users.

The Contractor is required to be incorporated in the United States, possess and maintain throughout the performance of the contract a physical address in the country, and conduct all primary registry services in the United States. The Contractor is precluded from charging the U.S. Government for the .us domain services, but is permitted to establish and collect reasonable fees from third parties for performance of the contract requirements, after approval by the U.S. Government.

The remainder of the paper provides additional detail on the obligations of the ".us" operator and on the re-delegation process.

### **Doc 38: Burkina Faso**

The Third African Telecommunications Regulators Network Forum on Regulation of Telecommunications in Africa which took place in Ouagadougou, Burkina Faso, from 19 to 21 November 2002 emphasized in particular the management of domain names and addresses. The Forum recognized that it is imperative for ITU to undertake, from now on, a leadership role in the field of international cooperation towards the development and harmonization of policies in this key area.

In this respect, the Forum recommended:

- to ICANN, that it fully cooperate with ITU in the implementation of Resolution No. 102 of the ITU Plenipotentiary Conference, Marrakesh 2002;
- to African regulators, the implementation before the end of 2003 of a coordinated strategy for the defense of their interests regarding ICANN, in coordination with ITU, namely the award and reclamation of domain names (ccTLD); and the creation of, at least, one routing server in Africa.

### **Doc 39: Switzerland and Switch**

In May 1987 researchers of the Swiss Federal Institute of Technology (ETH), Zürich, requested the entry of the "CH" TLD in the IANA WHOIS data base. On 20 May 1987 this topographic TLD was added as 14<sup>th</sup> ccTLD to the IANA WHOIS data base together with corresponding contact information. The IANA function at that time was performed on behalf of the US Department of Defense under the ARPA contract. In May 1987 no formal requirements existed for management of TLD's.

In October 1987 the foundation of the private sector SWITCH was established in order to develop and maintain the Swiss education and research network. Founding members were the Swiss government (Federal Department of Home Affairs) and eight cantons with universities. Management of the "CH" TLD was subsequently transferred from ETH to SWITCH and the entries in the root data base were modified accordingly. The first registrations of second level domains under "CH" were performed by SWITCH in early 1988.

In November 1987 RFC-1034 was published, describing technical details of the Domain Name System (DNS). The first document devoted to the management of "delegated" TLD's, RFC-1591, was published in March 1994 and this RFC is since then the basic document for the relationship

between the entity performing the IANA function and a TLD registry. Its successor, ICP-1, published in 1999 by ICANN, was never formally approved by the registries of “country code” TLD’s.

In the beginning, domain names were registered by means of e-mail, fax messages or even phone calls from registrants and entered in the then commonly used ASCII application form employed for both domain name and IP address allocation. By the end of 1995 1’300 domain names were registered under “CH” and it was felt necessary to enhance the system by introducing a liberal policy, registration software for fast machine-controlled non-discriminatory and well documented registration, websites, where registrants could apply for names and maintain them, and finally by introducing a charging system for each registered domain name. The new liberal registration policy was praised at its introduction as more advanced and better reflecting the important principles of equal treatment than policies by other registries. Para. 3 of all registration policy versions state that “any entity may register domain names, independent of the location of the entity. It is, however, recommended to register or reserve second level domain names below CH and LI top level domains only for entities located in said countries”. Fees for registration services have been decreased several times since 1996.

Due to the explosive growth of the Internet in Switzerland since 1996 – by the end of 1999 170’410 domain names were registered under “CH” – further improvements were made: user identification numbers, passwords and a new data base system as early measures to provide registration and modification security. Many more enhancements were made since then; a registration system is in constant need to be adapted to the latest developments.

Currently (as per February 2003), more than 500’000 domain names are registered under “CH”, seven name servers are resolving “CH” second level domain names worldwide (3 in Europe, 2 in the US, 1 in Australia, 1 in Argentina) and SWITCH customer care personnel communicate in three official languages (French, German and Italian) and have additional language skills in English, Spanish, Portuguese and Serbo-Croatian. The number of registrations compared to the number of inhabitants in Switzerland (ca. 7 Million) exhibits a high “domain name density” and it is estimated that more than 1 Million hosts are connected to the Internet at this time.

Solving conflicts: no special or alternative dispute resolution process has been considered as necessary because

- Swiss public courts apply fast and cost effective administrative procedures and
- most disputes involve claimants and respondents residing in Switzerland and
- the number of disputes under “CH” is generally low.

Some of the reasons for having a very limited number of disputes have been due to the fact that applicants were warned prior to registration of possible disputes that may arise when an application for a “well known name” was received and due to the fact that Swiss community names were “screened” by the registry since early 1997. The “screening” procedure usually requires a written confirmation submitted to the registry by the authorities of the community concerned. Such a “sunrise period” for community names has been felt as absolutely necessary.

SWITCH is a founding member of CENTR and the Worldwide Alliance of Top Level Domain (wwTLD) – this group was established in Geneva in 1998 –, a supporting member of ICANN and is participating in many other European and international organizations, both policy and technical standard settings bodies. It is anticipated that SWITCH will also become a member of the future ICANN ccNSO.



Any TLD registry has to rely on the IANA function for maintaining the entries in the TLD WHOIS data base and on the root name server operators for keeping the Domain Name System operational. Additionally, registries of the private sector need support from the local Internet community (LIC) since it is commonly understood that the authority of a registry is derived from the LIC.

#### **Doc 40: ICC**

We would like to note the critical importance of the technical co-ordination of the Internet to all of our members given that an increasing amount of their business is conducted over it. In that regard, the smooth and stable functioning of the domain name system, including ccTLDs, especially with the increasing registrations within ccTLDs, is essential to ensure the Internet continues to be a viable medium for commerce. ICC's long-held positions vis-à-vis the technical coordination of the Internet and domain name administration remain relevant.

ICC has been a supporter of the Internet Corporation for Assigned Names and Numbers (ICANN) since ICANN's inception. ICC recognized early on that the Internet would be the driving force behind global electronic commerce, and ICANN's stability and security are key to the ability of the Internet to provide a platform for business. Consequently, ICC has long held that business should have a significant role in the formation of policy for technical management of the domain name system. Technical coordination of the Internet and policy matters directly related to it, for example allocating IP addresses, managing the domain name system, and other ICANN functions, are best driven by the private sector. ICANN, with its balanced representation, is the appropriate organization to fulfill these functions. As such, ICC places high importance on ICANN concluding mutually beneficial relationships with key operators, including ccTLDs, regional Internet registries, and root-server operators, given the importance of their practices and policies to ICC members.

An effectively functioning and accountable ICANN is the best means of ensuring private sector leadership. Governments and inter-governmental organizations should continue to support ICANN through the Governmental Advisory Committee (GAC). ICC recognizes and appreciates the ITU's efforts, through its participation in the GAC, to bolster the existing institution of ICANN. In this context, ICC urges the participants of the workshop to continue to work towards improving the stability and effectiveness of ICANN in the future.

#### **Doc 41: Industry Canada**

This paper provides a general overview of the process that led to the re-delegation of the .ca in Canada.

The management of ccTLD .ca was delegated to John Demco of the University of British Columbia (UBC) by Jon Postel of the Internet Assigned Numbers Authority (IANA) in 1987.

Since the .ca's inception and registration with IANA in 1987, John Demco managed the .ca domain space using the facilities and equipment of UBC. John Demco managed the .ca on a voluntary basis. He and his group allocated .ca domain names at no charge to users. The evolution of the Internet, the nature of the .ca policies at the time and the delay involved in obtaining a .ca registration (about a week) relative to other DNS registries such as .com, generated widespread dissatisfaction within the Canadian Internet community.

In 1997 John Demco, UBC, the government of Canada and other interested parties recognized the need to revitalize the .ca domain space in order to maximize the public benefit. At the Canadian Internet community's annual conference, discussions of reform led to the formation of the Canadian Domain Names Consultative Committee (CDNCC) to address the transition from the current management of the .ca domain to a 'more commercial type of operation'. Following a public

consultation, the CDNCC recommended that a private sector, not-for-profit corporation be set up to take over the administration of the .ca from UBC and John Demco.

In 1998, the Canadian Internet Registration Authority (CIRA) was incorporated as a not-for-profit corporation with the intention of managing the .ca domain space in the public interest.

In 1999 a letter was sent to CIRA and signed on behalf of the government of Canada by the Assistant Deputy Minister, Spectrum, Information Technologies and Telecommunications of Industry Canada (the March 11 letter). In this letter, the Canadian government recognized CIRA as the new administrator of the .ca. It also set out the general principles and structure pursuant to which it expected CIRA to administer the .ca domain space. The general principles are:

1. conducting CIRA's activities in an open and transparent manner that ensures wide public access to all relevant information;
2. following fair and sound business practices;
3. ensuring an appropriate balance of representation, accountability and diversity on the Board of Directors for all categories of stakeholders;
4. applying for domain names being as quick and easy as applying for domain names in other top level domains, and priced competitively;
5. reducing conflicts between persons granted domain names and other rights holders, including trade-marks or business names; and
6. administering a system that facilitates and encourages entry for new players including registrars.

In May 2000, UBC, CIRA, and the government of Canada signed the Umbrella Agreement wherein the parties committed to providing an orderly transition of the management of the .ca domain space from John Demco and UBC to CIRA. Included in the Umbrella Agreement were the following statements:

1. UBC relinquishes any interest arising from its operation of the .ca domain space, and CANADA in turn designates CIRA to manage, operate, and control the .ca domain space in accordance with principles for the public interest described in the March 11 letter.
2. CIRA is to be recognized as having the exclusive authority to operate the top-level domain servers for the .ca domain.

The agreement achieved by UBC and CIRA recognizes the .ca domain space as a key public resource for the benefit of all Canadians.

The Umbrella Agreement was structured so that the delegation of authority to operate the .ca comes to CIRA from ICANN rather than the government of Canada. The agreement designates CIRA to operate or cause to be operated the .ca domain space in accordance with the principles and structure set out by the government of Canada in the March 11 Letter and in accordance with other principles, being in the public interest and being reasonable, as the government of Canada may, from time to time, set.

In October 2000, a letter was sent to ICANN on behalf of the government of Canada to formally designate CIRA as the Government of Canada's designee to be the .ca delegee. CIRA assumed its responsibilities as of December 1, 2000.

CIRA has been able to establish a more market-oriented approach to the registration of .ca domain names. In December 2000 there were 60,000 active names, today there are around 300,000. This represents an increment of 400% for that time period.

The paper provides details on CIRA policies and operations.

#### **Doc 42: AFNIC**

A sub-division of AFNIC, called the Collège International (CI) conducts activities for developing countries, in particular:

- Training:
  - Training trainers in information technologies
  - Models for NIC activities, including technology transfer such as software for registry operations
  - Development of multimedia tools for trainers
  - Virtual campus and remote training platforms.
- Operational support when taking over a ccTLD:
  - Presentation of the AFNIC organizational model
  - Technical support

The paper contains details on AFNIC, its membership, and partners, which include private organizations and inter-governmental organizations.

The CI intends to expand its activities by developing a collaboration with appropriate national and international bodies, in particular, UNESCO, ITU, and the CEA.

#### **Doc 43: OECD**

This document summarises a report which aims to provide comparative information on the administration of domain names in the 30 OECD countries as an aid to policy makers considering these issues. The main report will be considered for declassification by the OECD's Information, Computer and Communications Policy (ICCP) Committee which will be held on March 3 and 4, 2002 and the final version of the paper will be available soon after.

The number of domain name registrations is dramatically increasing. The major gTLDs grew from 17.4 million in July 2000 to 28.7 million in July 2002. Much bigger increase has been seen in the ccTLDs in OECD member countries. The ccTLDs registrations in the OECD member countries more than doubled from 6.7 million to 15 million.

In the OECD countries, most registries are non-profit organizations, which are usually formed by ISPs and Internet related organizations. There are some ccTLDs which are run by academic or government organizations (Finland, Mexico, Switzerland and Turkey). Private companies administer the ccTLDs in Japan and the United States.

Some 18 registries out of 30 OECD member countries have direct sales to the public. In this case, registries take roles of registrars. Some 6 registries among 18 accept registrations from registrars. The rest of 12 registries do not sell domain names. They put clear distinction between registries and registrars.

The gTLDs are operated under rules set by ICANN based on the Registry Agreement between ICANN and Registry. On the other hand, the ccTLDs are separately operated under rules of each ccTLD. In order to grasp an image of ccTLD administration, four policy issues are focused.

- Whether there is a local presence or related requirement to qualify for the right to register a domain name.

- Whether there is a limit in the number of domain names for which any single entity can apply.
- Whether there is an explicit policy in regard to trademark issues.
- Whether a WHOIS database is publicly available.

### ***Location requirements***

About Location Requirements, the registries of 17 ccTLDs in OECD member countries have location requirements and some 13 countries have no location requirements. Among 17 ccTLDs, some 11 ccTLDs impose nationality requirements and 12 ccTLDs impose local address requirements.

Nationality requirements mean that applicants, when acting in a private capacity, must have the same nationality of the country where they want to register a ccTLD domain name. For applications, which are not made by individuals, such as for organizations or corporations, the requirements generally specify that the entity must be registered under relevant laws of the country. Local address requirements mean that applicants must have legal and existing residency in the country.

### ***Application limits***

When the OECD last looked at comparative rules in this area among OECD member countries in 1997, some 18 ccTLDs had number restrictions on registrations. By 2002, some 26 ccTLDs, this number includes ccTLDs which partially allow unlimited registrations, have no application limits. In Greece, Korea and Netherlands, which partially allow unlimited registrations, private applicants are allowed to have only one domain name, but organizations can have unlimited domain names.

### ***Trademark policy***

All ccTLD registries in OECD member countries provide some trademark policies which indicate basic stance of registries toward any conflicts concerning domain name registrations.

The most common rules for domain name registrations are “first come, first served” basis. Therefore, most of registries in OECD member countries explicitly stipulate that registrants must take all responsibilities related to trademarks and other third party rights in domain name registrations. It is the responsibility of applicants to check they do not violate any intellectual property rights or any other rights.

The Australian ccTLD registry “.auDA” provides some guidelines for proper domain names. The registered domain names must (i) match the name of the registrant; or (ii) be an acronym or abbreviation of the name of the registrant; or (iii) be otherwise closely and substantially connected to the registrant.

JPRS, the Japanese registry of “.jp”, introduced a preliminary registration application system in order to prevent possible domain name disputes, when the general-use domain name “.jp” was introduced for the first time in 2001, (in addition to the existing second-level domain names.) During the one month preliminary registration period, copyright holders of trademarks and registered names besides existing domain names holders under second level domain names could apply for new domain names prior to other general applicants.

### ***Information availability by WHOIS***

The WHOIS service enables inquirers to find contact information on registered domain names. The information provided by the WHOIS services can define who is responsible for the registered

domain names. The clear indication of responsibility can help to resolve any technical problems and this information can be used in relation to a number of areas such as consumer protection in electronic commerce and other Internet transactions, trademark disputes, and other legal issues.

For the gTLDs, ICANN asks its accredited registrars in the Registrar Accreditation Agreement to provide the WHOIS services which enable public access to data on registered names. Because the ccTLDs are not directly subject to rules created by ICANN, information availability policies regarding contact information for the ccTLDs depend on each authority of the ccTLDs. However, in all OECD member countries except Portugal and Slovak Republic, registries provide the WHOIS service. Registries usually provide the WHOIS service on their Web sites as the first step for applicants to determine the status and availability of domain names. In Portugal, the registry does not provide WHOIS service because of privacy issues. In Slovak Republic, the registry provides the list of registered domain names instead.

Although the WHOIS service is available in most OECD member countries, there is the difference in information availability. Information availability was compared based on items to be provided by gTLD WHOIS. The big difference was found in contact information which contains personal information because of privacy issues. Just over 10 million domain names which are about 70% of total domain names in OECD countries have contact details on the WHOIS databases.

### ***Privacy regulations***

The administrative and technical contact information that defines responsibilities for any registered domain name may be useful and important for the security and the stability of the Internet. However, there are also privacy issues to be considered and some countries do not allow personal data to be publicly available on the WHOIS based on their legal requirements (e.g. Australia and Mexico). And some OECD countries have introduced different deals between private registrants and business registrants in the disclosure of the WHOIS data (e.g. Denmark and United Kingdom).

### ***Accuracy of WHOIS data***

There is a strong concern for the inaccuracy of the WHOIS data from various fields, such as taxation, consumer policy, security, law enforcement. Inaccuracy WHOIS data is caused by fictitious registration by registrants. Fictitious registration is caused by two types of registrants. One is fictitious registrant such as a cyber squatter and an Internet fraud, and the other is a private registrant who does not wish to reveal their personal data because of privacy concerns.

Against those inaccuracy or incomplete registrations, most registries of the OECD member countries can take some actions. They are requesting accurate information from applicants and they can cancel domain name registrations in the worst case. But the problem is how to check and find them. As an example, the Australian registry “.auDA” verifies the registered data periodically.

## **Doc 44: Syrian Arab Republic**

The responsibility for root directories and domain names should rest with a suitable international organization and should take multilingualism into consideration. Countries’ top-level-domain-names and Internet Protocol (IP) address assignment should be the sovereign right of countries. The sovereignty of each nation should be protected and respected. Internet governance should be multilateral, democratic and transparent and should take into account the needs of the public and private sectors as well as those of the civil society.

The Syrian administration believes that ITU is the only suitable international organization to deal with this matter, based on its successful experience with similar issues.

Also, the Syrian administration was surprised to learn, from reports on E-Mail discussion lists, that the Internet Corporation for Assigned Names and Numbers (ICANN) may require that a ccTLD sign a contract with ICANN as a pre-condition of any ICANN act—recognition of a re-delegation or even updating the name server records pointing at the ccTLD's servers—and that this precondition would "promote the stability of the net".

In the Syrian administration's view, such a proposal has nothing to do with stability. On the contrary, we believe that any cross-linkage and cross-leverage of ICANN and the Internet Assigned Names Authority (IANA) is not justified.

We would appreciate it if participants would clarify the issue, and whether the signing of such contracts is necessary, and if so what are the justifications for that.

We would also appreciate it if this workshop could lead to a series of steps towards the fulfillment of ITU's role in this domain, taking into consideration ITU Resolution 102 (Marrakesh, 2002), and the full independence of national authorities dealing with this matter.

#### **Doc 45: Verisign**

Located near Fiji in the South Pacific is a collection of nine atolls that make up the nation of Tuvalu. Having gained its independence in 1978 and joined the United Nations in 2000, Tuvalu has no measurable natural resources, other than fish, that can be developed to support education, health care, or the development and provision of basic utilities and services. With limited infrastructure or services to attract tourism, the nation has historically attracted fewer than 1,000 visitors each year. Tuvalu's major source of income has come through the licensing of fishing rights, primarily to companies from Asia, Australia and the United States.

With the advent of the Internet, Tuvalu's outlook for economic development improved significantly thanks to the nation's partnership with the .TV Corporation (currently a part of VeriSign) for the development of the .tv top level domain. This public-private partnership has produced startling results that have had a far reaching impact on the Tuvaluan community. The paper lists the most significant results.

To effect its partnership, Tuvaluan government officials serve in a consultative role and have established a .tv Oversight Board to undertake that responsibility. Consultation rather than regulation is a central principle for oversight of the top level domain. The VeriSign - .TV Corporation reports to the government on a quarterly basis, which reports include summaries of financial results, domain name sales numbers, a summary of industry trends, marketing and promotional plans, and other pertinent information.

However, the VeriSign - .TV Corporation, as the government's commercial partner, is left to make all relevant business decisions such as how to market .tv domain names, pricing and other strategic decisions. This carefully measured balance between government and private interests provides each party with appropriate incentives to maximize the value of the .TV name and brand, and provides a favorable environment for substantial private investment by the VeriSign in the partnership.

The Tuvalu model does not fit all ccTLD's; nor does it fit all ccTLD's from developing countries. But it has important lessons for how a public-private partnership in the DNS can contribute to economic growth and help close the digital divide. In most cases however, governments in developing regions can and should play an important role in promoting public-private cooperation by taking a page from the Tuvaluan government's basic perspective. Under a well-defined agreement with a trustworthy partner, a government can use the DNS to promote economic growth. In doing so, it should avoid unnecessary regulations that are, in reality, barriers to private investment, and limit its role in the operation of a country code top level domain to that of

consultant and advisor. Business and strategic decisions can be delegated to a reliable commercial partner, with the stated intention of maximizing the value of the country code top level domain and providing the best service possible for end users and consumers.

#### **Doc 46: NOMINUM**

The robustness and reliability of the Domain Name System depends on a simple rule: there should be no single point of failure. In addition, the Internet Engineering Task Force (IETF) has produced recommendations on the operation and configuration of name servers to enable operators and technicians to provide a stable DNS infrastructure. The objective of this document is to analyse how the DNS infrastructure for the country code top-level domains (ccTLDs) meets these requirements.

The raw data for the survey was collected over the weekend of Feb 14-17th 2003. The delegation for each ccTLD was checked from the root servers, giving a list of the name servers for each ccTLD. Those servers were in turn queried to find out more about the ccTLD(s) that they served. The survey checked all 243 ccTLDs.

A packet tracing tool was then used to find the path packets took to reach those name servers from a computer based at the London Internet Exchange, LINX. This is a very important communications hub for the internet with connectivity to most carriers and major Internet Service Providers. The object of this was to find out if there was an excessive concentration of ccTLD name servers at one location or if a ccTLD's servers were in one place, creating a single point of failure.

One of the most startling initial findings was that the names of 18 ccTLD servers did not exist in the DNS! In other words, approximately 2.5% of the ccTLD name servers had names that could not be looked up. Essentially the ccTLD hostmaster is advertising the presence of a name server that they should know does not exist. Since those names could not be looked up, those "phantom" name servers could not be queried, assuming they even exist under some other name. This is a glaring error which simply should not happen. It may be understandable when someone new to the DNS sets up a name server and registers a domain name for the first time. However it should never occur in ccTLDs because these important domains should not be operated by naive administrators and any changes to the ccTLD setup should be carefully checked.

Although this is a serious and fundamental error, it is fortunately not a mission-critical one. All of the ccTLDs that advertise these phantom name servers also advertise name servers that do exist and serve the ccTLD. So service for the ccTLD is still available although it will be impaired by the existence of these phantom servers that cannot be queried. The DNS will treat these as unresponsive name servers. The DNS protocol has mechanisms for handling unresponsive servers, something that contributes to the overall robustness of the DNS. However keeping track of these unresponsive servers means more work for everyone else's name servers, extra overheads and longer lookup times.

Sadly, one ccTLD is in a very bad way. It appears to have 4 name servers. Only one of them is correctly defined. The other three are listed as dotted decimal strings -- presumably their IP addresses -- rather than valid host names which the DNS requires. This ccTLD has a major single point of failure. If its only correctly named server becomes unavailable, the ccTLD will disappear from the internet.

Another 10 of the name servers do not have host names as required by the DNS protocol. Instead they are present as CNAME records (nicknames). This is illegal, though most name servers tolerate this error. However using CNAMEs instead of hostnames can cause name resolution problems. Again, this is a basic administrator error which should not occur in an important DNS zone like a ccTLD.

It would be expected that there would be no mismatches between the root and a ccTLD over the ccTLD's name servers. The reality is very different. 155 of the ccTLDs do not have the same NS records for the TLD as in the root, their parent zone. In other words, 64% of the ccTLDs have mismatched delegation information between themselves and the root.

There is no excuse for this. In a well-maintained zone, mismatched delegations simply would not be allowed to happen. These errors generally result from DNS administrator error. However for ccTLDs there is a mitigating factor. Changes to a ccTLD delegation involve updating the root zone and this can only be done after the ccTLD makes a request to ICANN. Many ccTLDs are in dispute with ICANN which has created a stalemate. ICANN won't alter ccTLD delegations in the root unless the ccTLD signs a contract with them, something most ccTLDs are reluctant or unable to do. Although this impasse could explain why there are so many mismatches, it does not present a valid excuse in most cases. The ccTLD should not have changed their NS records unless that change was reflected in the root zone.

Fortunately, most of these mismatches are not serious. The ccTLD's set of name servers generally turns out to be a superset of those listed in the root zone delegation for the TLD. This is harmless from an operational perspective. Even so, this is damaging because it suggests that the internet root and ccTLDs cannot keep this simple and fundamental information properly synchronised. The implications of this could be far-reaching.

A lame delegation in the DNS is a serious problem. This occurs when a server that is supposed to answer authoritatively for some zone does not. This is always caused by administrative error. Unfortunately 43 ccTLDs had 1 or more lame servers. In the case of 2 ccTLDs ALL of their name servers were lame. A further 8 ccTLDs had more than half of the servers lame. Clearly, some ccTLDs are not taking proper care of their delegations. Put simply a zone should not have NS records pointing at non-authoritative servers. Lame delegations for ccTLDs would not occur provided this simple rule was followed by the administrators of these important domains. This is a problem that needs attention, perhaps a ccTLDs, ICANN and other interested parties jointly developing and enforcing a code of conduct.

Name servers for a ccTLD should be configured to be authoritative-only. Since they should only be queried by other name servers, there should be no reason for a ccTLD server to process recursive queries. These lookups should of course be handled by the name servers that query the ccTLD name servers. Surprisingly, almost half of the Internet's ccTLD name servers have recursion enabled. 371 of these servers will process recursive queries. This means 47% of the ccTLD servers are needlessly exposed to cache poisoning, and can spread any bogus data they get from querying other name servers. Furthermore those 371 servers could easily be overwhelmed by recursive queries, preventing them from answering genuine queries for the ccTLDs they serve. This needs to be fixed.

Zone transfers are the usual mechanism in the DNS to propagate zones from the master (primary) server to its slaves (secondaries). As its name suggests, this mechanism involves taking a complete copy of the zone.

Although this is an everyday part of the DNS protocol, ccTLDs should impose restrictions on who is permitted to perform transfers of their zone data. Out of 243 ccTLDs, 140 permit zone transfers. Within the ccTLDs that permit zone transfers, the rule or policy is usually inconsistent. Some of the name servers for a ccTLD allow zone transfers, others don't. This is probably explained by the servers being under different administrative control and the ccTLD not establishing and enforcing a consistent policy with all of their slave (secondary) servers.

The consequences of this finding are disturbing. Controls on zone transfers tend not to be used by most ccTLDs. And even when they are enforced, it is usually on a per-server rather than a per-



ccTLD basis. Given the potential for abuse from open zone transfers, this seems like a vulnerability waiting to be exploited.

Another concern is the fact that most ccTLDs seem to be running versions of BIND version 8 that have known security problems.

When ICANN recently created the new gTLDs, it insisted that the name servers for these gTLDs were located in different address prefixes assigned to at least 2 Autonomous System Numbers. The rationale was that if there was a routing problem with one ASN, there would still be another that was announcing routes to at least some of the gTLD's name servers. It seems strange that this requirement is not required or even recommended for ccTLDs.

The paper recommends that monitoring tools be put into place, service level agreements be concluded and steps be taken to protect against denial of service attacks.

### **Doc 47: Australia**

Australia's experience in the development of the Internet and particularly within the .au domain is similar to that of many other countries in that it was managed on a voluntary basis for a long time. This arrangement served Australia well in the Internet's formative years. However, over time, as the Internet became a more important tool for businesses and others, pressure came to bear for a more robust and scalable management system for the .au domain.

In Australia, this took the form of an industry self-regulatory regime. The original push for a more formal process came about in 1996, and it has taken almost five years to get to where we are today. The reasons for this are many, but the primary reason was that this was a new technology which evolved over time to have significance for many other stakeholders than originally intended. The change from the legacy arrangement to self-regulation has met with many challenges. Australia's first attempt at self-regulation was championed by industry stakeholders, but for many reasons was ultimately unsuccessful. Government assistance was sought to facilitate the transition, and this was ultimately achieved in collaboration with key stakeholders including industry and user groups. It is important to realise that, while the Australian government has played key roles in the creation of auDA and the redelegation, it only took on these roles after this first attempt at industry self-regulation failed.

This paper provides a historical analysis of the development of the Internet in Australia and highlight the move to a self-regulatory environment and the subsequent redelegation process of the .au ccTLD from the previous delegate, Mr Robert Elz, to auDA. Australia was the first country in the ICANN environment to go through the formal redelegation process and enter into a triangular arrangement between ICANN, auDA and the Australian Government. This achievement has been heralded by some but criticised by others for breaking ranks with the past.

Among the requirements of the new self-regulatory regime are:

- operate as a fully self-funding and not-for-profit organisation;
- be inclusive of, and accountable to, members of the Internet community including both the supply and demand sides;
- adopt open, transparent and consultative processes;
- aim to enhance benefits to Internet users through the promotion of competition, fair trading and provisions for consumer protection and support;
- establish appropriate dispute resolution mechanisms; and

- represent Australian Internet industry interests in the Internet domain name system at national and international fora.

Satisfied that auDA had met the necessary requirements, in December 2000, the Minister for Communications, Information Technology and the Arts, Senator the Hon Richard Alston, formally endorsed auDA as the appropriate entity to manage the .au domain space.

In June 2001, auDA wrote to IANA formally requesting the redelegation of the .au domain from the current delegate, Robert Elz to auDA. It was to be another four months before an Agreement with ICANN was signed on 25 October 2001. There were a number of reasons for the delay, among them was the reluctance of the current delegate to agree to the redelegation. ICANN was keen to afford Mr Elz the opportunity to outline his concerns. He was primarily concerned that auDA was not sufficiently representative of the Internet community and was of the opinion that if anyone was to take over the administration of .au in the immediate future it should be the Australian government. During this time, Melbourne IT wrote to IANA along similar lines, suggesting that the appropriate entity to hold the delegation was the Australian Communications Authority, the body responsible for the management of Australia's communications industry regulatory framework.

ICANN's CEO, Stuart Lynn, subsequently sought reassurances from the Australian Government on the ability of auDA to administer the .au domain space in the interests of the Internet community. The Minister for Communications, Information Technology and the Arts wrote to Mr Lynn reiterating the Government's support for auDA.

On 31 August 2001, IANA issued a report on a Request of the .au Domain Administration (auDA) for the Redelegation of .au Top -Level Domain. Under the proposal, auDA would undertake management of the .au ccTLD under appropriate oversight of the Australian Government (concerning national public-policy interests) and ICANN (concerning global technical-coordination interests).

On 4 September 2001, ICANN posted the proposed Sponsorship Agreement with auDA for public comment. On 10 September, following its public forum, the ICANN Board authorised the ICANN President to enter on behalf of ICANN the ccTLD Sponsorship Agreement for .au with auDA.

On 25 October 2001, auDA signed an Agreement with ICANN to formalise the transfer of delegation for the .au country code Top Level Domain (ccTLD). The Agreement set out the triangular relationship between auDA as the .au delegate, the Australian Government, and ICANN as the international domain name governing body. This agreement was the first such formal document establishing a relationship between a national Government, ccTLD administration and ICANN. This was based on the GAC Principles for the delegation and administration of Country Code Top Level Domains.

The move to an industry based self-regulatory regime seems to be working well at this time, and auDA has certainly made significant progress since its inception. However, it may be too soon to make a definitive statement about its success, unfortunately only time will tell.

The introduction of competition into the .au domain space is currently taking place, and auDA's success will be largely measured upon whether this transition is indeed workable and delivers the anticipated benefits of cheaper prices, more choice and better quality of service.

While the Government is confident in auDA's ability, it does have a fall back position. On 7 December 2000, the Parliament passed amendments to the *Telecommunications Act 1997* and the *Australian Communications Authority Act 1997*. The amendments clarify the powers of the Government in relation to "electronic addressing" services such as Internet domain names. Specifically, the amendments clarify existing provisions in the *Telecommunications Act 1997* for

the Australian Communications Authority (the ACA) and the Australian Competition and Consumer Commission (the ACCC) to "declare" and "direct" a manager of electronic addressing.

It also introduces a new provision into the *Australian Communications Authority Act 1997* that would allow the Minister to instruct the ACA to assume direct responsibility for an electronic addressing service, should self-regulation prove inappropriate at any time in the future.

The powers embodied in this legislation are only likely to be invoked if industry self-regulation was a failure in Australia. In this context, the Australian Government remains committed to the principle of self-regulation.

#### **Doc 48: Hong Kong S. A. R., China**

This paper aims to share the experience in redelegating the administration and assignment of Internet domain names under ".hk" top level domain in Hong Kong.

The Joint Universities Computer Centre (JUCC) in Hong Kong started its role as the administrator of the ".hk" Internet domain names in 1990 after its predecessor had registered the country-code top level domain, i.e. ".hk", for Hong Kong.

The JUCC provided registration services of ".hk" under five second level domain categories, i.e. .com.hk, net.hk, edu.hk, org.hk and gov.hk. A one-off fee was charged for each application for registration of new domain names or modification of existing domain names. No annual renewal fee was required. However, an organization was allowed to apply for only one domain name which was non-transferable.

With the rapid development of the Internet and electronic commerce in Hong Kong, the number of new Internet domain names registered in 1999 showed an increase of 160% compared with that in 1998. To facilitate the increasing Internet activities in Hong Kong, there were suggestions that greater flexibility should be allowed in the domain name registration system. Views were also expressed as to whether the JUCC was able to adequately represent the interests of different sectors in Hong Kong in discharging the administrator function for ".hk" domains.

The paper provides details of the redelegation process. The critical success factors were:

- Full commitment of the Government
- Community support for the redelegation
- Involvement of stakeholders
- Nature of the new corporation
- Financial compensation to original administrator
- Financial resources
- Initial governing board
- Means of transfer
- Dispute resolution mechanism
- Reregistration of domain names

#### **Doc 49: Vittorio Bertola**

The Internet has gone through very different stages in its growth, but it has now become a vital instrument in everyday life in all countries of the world. Whether it's for business, for social activities, for free speech and political discussion or for national security, the life and the

wealthness of a nation depend more and more on its computer networks, and computer networks are now mainly relying on the worldwide TCP/IP environment.

This naturally creates an alliance between very different types of Internet users in each country – individuals, corporations, governments... – to keep the network effectively operational. But this also creates a national security problem in ensuring that its administration and functionality does not depend on foreign resources, and, more generally, an increasing need by national governments to be able to impose and enforce legislation on online activities – a need which conflicts with the intrinsic cross-border nature of the Internet.

This, in my opinion, is the main cause of a drive to enforce a concept that until a few years ago was unknown or even dismissed as dangerous to the network itself by its (then mainly technical) population: the concept of “national digital sovereignty”.

In this view, also the role of a ccTLD manager is dramatically changing. At the origins of the Internet, a ccTLD was just a two-letter string kindly delegated by an US entity to more or less whoever it liked. In the years of the “Internet bubble”, the biggest ccTLDs were put under pressure to keep the pace of the development of national Internet usage, and thus changed from amateurish free-time activities to dedicated and efficient professional organizations. But now, as politicians and governments get more and more interested in the Internet, ccTLDs often start to be considered as the natural coordination point for the technical administration of the national Internet activities, and to be requested not just technical and operational efficiency, but also “political” efficiency in acting as a widely supported policy making body involving all stakeholders (or less nicely, depending on the country’s political attitudes, they are sometimes being required to become an appendix of the national government).

As a consequence, the ccTLD has become a corner stone of a country’s authority over its vital telecommunications infrastructure, not just because of its practical importance, but because it is the symbol of the country’s identity in the global Internet, and the rallying point for its active Internet community.

Under this light, it is clear that the present configuration and policies of the root level administration of the Internet are inadequate to the new situation. Until now, ICANN did not take this change into account; in many respects, it is behaving as if the Internet was still an US research project, owned by the US Department of Commerce, just with Dr. Cerf in place of Dr. Postel. Independently from what lawyers may say about the actual ownership structure of the Internet, this is not any more true or acceptable at the political level; and while this does not mean that ICANN is useless or illegitimate, it means that it has to change its attitude towards the rest of the Internet.

Due to the very nature of the Internet, its administration requires the awareness that diversity is its main value, that only policies on which there is general consensus can be widely adopted, that central regulation needs to be kept at the minimum; and this is not just a question of regulations or organizational structure, it is a question of mental attitudes.

On the other hand, the initial idea about ICANN – that the Internet has to be ruled by a specific private entity in which all stakeholders are represented, rather than directly from governments – is still valid. Some have proposed that the management of the root server system is devolved to an international governmental organization. Now, while transformation of ICANN from an US corporation into an international organization is highly desirable and should happen as soon as possible, I think that centralizing too much power in the hands of the governments and of intergovernmental structures would again miss one important lesson we learned from the history of the Internet.

Often, government officials see the direct involvement of the Internet community in its administration, especially if with direct voting power, as a remainder of amateurish times. They say, *“we don’t let car makers or car drivers vote on traffic regulations, so why we should let ISPs and Internet users vote on Internet regulation?”* But in this, they fail to realize that it’s exactly this sort of short-circuit direct chain between the consumers, the industry, and the market which has allowed the Internet to expand at speeds previously unknown, and to create new activities, new opportunities, new jobs, and new economical wealthness with it, widely spread across the society. Computer networks deployed top-down by public monopolies were never successful or able to create diffuse wealthness and open communication; the unique characteristic of the Internet model, where consumers can instantly become producers of new content and new technology without having to go through a centralized regulator, though creating new and difficult problems in terms of law enforcement and security control, has also been provenly creating invaluable new opportunities for mankind, from the very practical to the very high-level fields of socio-economical interaction.

The paper suggests that ccTLD operators should be non-profit organizations representing (and accountable to) all components of the local Internet community, and it further suggests developing relations between the regional at-Large bodies and ccTLD operators.

### **Doc 50: Sudatel**

In 1996, Internet was introduced in Sudan by the Sudan Internet Services Co. Ltd. [Sudanet]. With 128Kbps Bandwidth capacity. In early 1998, the Sudan Telecom Co. Ltd. [Sudatel] introduced it’s Internet Service in the country as a value added service to it’s basic fixed telephony services. With 265Kbps Bandwidth capacity. In June 1998, an agreement was reached between Sudatel and Sudanet. By this agreement, Sudanet becomes the only ISP in Sudan. In Nov 1999, Sudatel became the only PoP in Sudan with 2Mbps form EMIX. Sudatel opened it’s Internet service provisioning to other potential service providers, the enterprise and universities sectors using it’s existing data communication infrastructure.

In 1996, the responsibility of .sd was delegated to Sudanese private company called Sudan On-Line, which was operated by a Sudanese citizen located at the United States. The domain was inactive since its delegation. Partially due to the lack of internet service and community then, and partly due to the presence of the operator in a foreign country away from the local Internet community. As the Internet service became more and more common to ordinary people, universities, enterprises and as the level of awareness increased, both, within the local community and the different government bodies and authorities. Number of bodies started showing interest in acquiring the .sd operations responsibilities, some for the good, some for the evil ! Early 2001, a non-profit, non-government a technical professional body was formed. Called Sudan Internet Society [SiS].

The main objectives of SiS was to increase the Local Internet awareness, help develop policies, Internet technologies and suggest some regulations with respect to the Internet usage in the country. This organization was supported by all telecom operators, ISP’s, the regulatory, the government, as well as the local community. SiS made re-establishing the .sd services one of it’s strategic objectives. Early 2002, SiS started contacts with ICANN as a first step towards a request for the .sd management re-delegation. The first meeting between SiS and the ICANN management was held in Tunisia during a conference that was held in Tunisia in April 2002. The correspondence between SiS and ICANN continued from then until July 2002 in order to prepare all the required documents and prove the local community as well as the government support, the technical proficiency to operate the .sd ccTLD.

A re-delegation template was submitted in August 2002. The second meeting between SiS and the ICANN management was held in shanghai during the ICANN Shanghai meeting, where an MoU was signed. The .sd was re-delegated by ICANN, IANA to SiS operation in Dec 2002.

Initially the government was not very much aware of the importance, of the .sd ccTLD. As the internet awareness started growing within the local community, the government started realizing it's role towards the technology revolution that is taking place in the country in particular and the region in general. The Sudan Internet Society, was able to gain the government support as a .sd operator, and hence, one of the SiS strategic objectives was to keep the government as well as the local internet community aware of all the local and International developments in the Internet Area. The government is fully represented in the .gov.sd name space reservation and allocation through the National Information Center, which is its IT body Sudan Ministry Council. The local government does not try to impose any restrictions that hamper the technical revolution within the country, instead it opened the market for private sector competition with the supervision of an independent regulatory body (i.e. NTC).

The paper contains extensive detail on .sd operations and policies.

### **Doc 51: CENTR**

CENTR members welcome the opportunity of the workshop arranged by the ITU Telecommunications Standardisation Sector (ITU-T) on 3 – 4 March 2003 in Geneva, to share their views on the administration of the domain name system (DNS), within the global process of the reformed Internet Corporation for Assigned Names and Numbers (ICANN).

CENTR members are grateful that this ITU workshop provides a forum for interested parties to explore how the DNS sector operates, and identify how they can best contribute to the process.

The domain name landscape is diverse in many ways, from small to large operators, from strict to liberal policies, from academic networks to private companies. However, these operators are based on a number of key unifying principles.

Most importantly, all registries operate in a way that is accountable to the Local Internet Communities, reflecting the desires of local stakeholders in how their respective national resources are operated.

Beyond this guiding principle, there are commonly held views on most aspects of the industry.

As essentially a technical resource, standards on technical interoperability and deployment are paramount for the effective functioning of the DNS. ccTLD Managers work closely to ensure standards are developed, and adhered to, with operational policies that integrate with technical reality.

With differing regulatory environments, ccTLDs are also concerned with ensuring there is a stable framework in which they can operate their services. It is key to providing dependable services that ccTLD managers are not subject to arbitrary action beyond their control.

The success of the domain name industry is perhaps best illustrated by the low amount of attention it obtains from the public generally. European ccTLD Registries have reliably and dependably provided a stable and trusted resource that operates effectively. As a service that is literally taken for granted, we see one indicator of a well-functioning industry.

The paper provides references to more detailed papers published by CENTR.

### **Doc 52: Channel Islands Registry**

The paper briefly describes the Channel Islands and their constitutions. It notes that the Islands have never been part of the United Kingdom and that they have their own Parliaments, Legal Systems and Governments. The paper briefly describes the ccTLD Registry which manages the .GG and .JE domains, and further describes private sector mechanisms by which consultation takes place

between the Channel Islands Registry and the Governments of the Islands in regard to the Islands' ccTLDs.

In mid-1996 the Internet Authority for Assigned Names and Numbers (IANA) agreed that the Channel Islands Registry would be set up and that the codes of "JE" (Bailwick of Jersey) and "GG" (Bailiwick of Guernsey) could be allocated.

The generally acknowledged terms and conditions for the creation of ccTLDs were, in 1994, embodied in an RFC (Internet Standards Document) known as RFC-1591.

It is the terms and conditions contained within RFC-1591 which describe the terms under which the Channel Islands Registry has operated since 1996, and remains so until it is mutually agreed otherwise between the Registry and whichever agency eventually takes over responsibility for the DNS root server system from the US Government.

The Registry, like most European registries is not a part of any Governmental agency. Yet at a very early stage it was determined that, with two ccTLDs representing four different and independent jurisdictions, a method of communication and co-operation between the Registry and the Insular Authorities would be highly desirable.

The CI-GAC was set up in 1997 by the Registry with invited representatives from two of the four Island governments. The other two Island Governments joined shortly thereafter.

Indeed, the Registry's Channel Islands Governmental Advisory Committee, while specifically for communication between representatives of the four Governments and the Registry has also proved a useful forum for an exchange of views on general e-commerce matters between the governments unrelated to domain name matters.

This does not mean that there is always total agreement between the Registry and the members of the Advisory Committee. For example, one of the Governments restricts the use of corporate names and has from time to time has sought to apply the same bias when considering matters relating to Internet Domain Registration without fully understanding the differences between company names and internet names. This has highlighted the importance of informing and educating all parties through such a consultation process.

The Registry has also benefitted from insights into public policy considerations from the Governmental members.

In early 2000, all four Island Governments were taking part in the Advisory committee, and it was decided to produce a formal document describing the the co-operation. This took the form of a Memorandum of Understanding which recognised the private sector nature of the Internet Registries and at the same time provided a formal basis on which the Island's Governments could fully participate in consultations regarding proposed domain name rule changes or other matters of common interest.

Like all ccTLDs, the secure and stable operation of the root server is of concern to both Registry and to the authorities.

The root server system is run well, and is run mostly by volunteers, some of which are outside the USA. The authoritative "A" root is, however, run by Verisign (Network Solutions) under a direct contract with the United States Government.

This essentially means that the Government of one country has *de facto* control over the e-commerce infrastructure of all other 240+ sovereign countries and territories and in theory (if not in practice) could affect or re-reroute internet names within any ccTLD.

Despite this fairly remote possibility, given the current stage of evolution of ICANN, it is considered preferable by many ccTLD Managers that the US Government does *not* hand over control of the root to ICANN as things stand today.

However it does not appear to be desirable in public policy terms for most sovereign countries in the medium- to long- term that a single country should have total control of the World Root , since this could lead to the possible perception that the operation of the authoritative World Root may favour that country's own economic interests, unconsciously or otherwise.

Therefore the most fundamental issue that still remains to be addressed is that of internationalising the operation of the A root server system.

### **Doc 53: ICANN GNSO**

The Council of ICANN's Generic Names Supporting Organization resolves:

1. to welcome the interaction of ICANN with relevant governments and inter-governmental entities (such as the International Telecommunications Union (ITU), the World Intellectual Property Organization (WIPO), the Organisation for Economic Cooperation and Development (OECD) and the European Union (EU) through the Governmental Advisory Committee;
2. to encourage governments and such governmental entities to consider ICANN as the primary venue to address Internet naming and numbering issues within the mission of ICANN;
3. to encourage and welcome governments and such governmental entities to attend and participate in ICANN's venues and meetings and to work actively within ICANN.

### **Doc 54: InternetNZ**

Operation of the .nz domain name space is not governed by any statute. The New Zealand Government acknowledges InternetNZ's responsibility in respect of .nz and the role it takes in ensuring its effectiveness. As such, the Government has not sought to introduce sector specific regulations, or control mechanisms in relation to the Internet in New Zealand.

The Government's general policies for the development of the Internet may be summarised as:

- The private sector should lead the development of the Internet
- The expansion of the Internet should be market and technology driven
- The Government supports the presence of a competitive, predictable, minimalist, consistent and technology-neutral legal and regulatory environment for the Internet
- There is an international dimension to many Internet issues such as jurisdiction and intellectual property rights that may need to be subject to international agreements.

The Internet Society of New Zealand, Inc (InternetNZ) has responsibility within New Zealand for the .nz domain name space. InternetNZ is a non-profit incorporated society, with membership open to all. Current membership of InternetNZ is representative of the range of sectors utilising the Internet,

Recent changes to the management of .nz have resulted in:

- a shared registry system (SRS) being implemented
- the position of Domain Name Commissioner (DNC) being established



- a committee being formed that has formal oversight of .nz matters. The DNC reports to the Chair of this committee.
- the establishment of a new registry company, trading as .nz Registry Services (NZRS), to operate the register
- a process to authorise registrars to enable them to connect to the SRS and offer registration and management services for .nz domains
- detailed .nz policies and procedures that establish rules and standards for how the .nz space will operate, with a clear reference to sanctions being taken should those be breached
- formal agreements being developed between key entities in the SRS
- more competition in the .nz market, and greater choice for registrants

The paper provides details of .nz policies and operations.

### **Doc 55: Elisabeth Porteneuve**

Who are ccTLD Managers? How many are they? When ccTLDs registration occurred? How it happen? What events are related to the ccTLD creation? Where are records of registration? Who is in charge of the custodianship of this patrimony of the world?

Were the assessments or public audits of the ccTLD IANA database made over time and published? Do we have any document assessing the status of the ccTLD IANA database when transferred from the SRI NIC to the NSFNET project, or later in 1993 from the NSF to InterNIC (NSI)? In the end of 1998 after Jon Postel passing away? In February 2000 when the first purchase order for IANA function has been sent by the DoC to ICANN?

Some of the questions above have answers, some could have, but the comprehensive ccTLD Book of Genesis, documenting registration of all 240+ entries does not exist.

The preamble to the ccTLD IANA function is related to the archives of the ccTLD IANA database. The ccTLDs cover the whole world. The ccTLDs' IANA database is the history of the Internet creation, part to the world patrimony. Without those fundamental records providing information on all past ccTLD history and all changes ever recorded no much trust can be built for the future. In addition to the duty and responsibility of keeping historical archives, the analysis of documents from ccTLDs registrations could be an extraordinary lesson on international deployment of the Internet, not less interesting than the discovery of continents and countries half millennium ago.

It is time to admit than the ccTLDs' issues will take time. The establishing and maintaining policies for the ccTLD IANA function is a complex and long term matter. While trying to imagine the structure for the "ccTLD IANA Maintenance Agency", we could take lessons from the ISO 3166/MA history and difficulties:

"In addition a mechanism for the maintenance of the new standard had to be developed because user acceptance for this kind of standard critically depends on its being up to date."

### **Doc 56: Internet Society of England**

ISOC England believes that at the time when the ICANN Board and staff are implementing the Reforms introduced at the ICANN Board Annual Meeting in Amsterdam on 15 December 2002, the US Department of Commerce has rightly concluded that ICANN is the organisation which uniquely provides and can, in the future provide, a seamless performance of the IANA functions with effect from 1 April 2003.

Bottom up policy development through the ICANN process and private sector self regulation is recognised by governments of more than [70] states that are members of the ICANN Governmental Advisory Committee as important elements in the organisation and management of global Internet resources. ISOC England are unaware of any compelling reason emerging through the ICANN process to distribute the IANA functions across a range of entities

ISOC England encourages the US Department of Commerce to conclude later this month that ICANN can and should continue to;

- coordinate the assignment of technical protocol parameters;
- perform administrative functions associated with root management; and
- provide overall responsibility for the allocation of IPv4 and IPv6 delegations of IP address space.

The opportunity of the award of a new Purchase Order at the end of March 2003 should nevertheless be taken by the Department of Commerce to stipulate performance evaluation criteria and service level targets for audit by the Department during the lifetime of the Purchase Order.

An assessment of ICANN's continuing management of the IANA function and whether it meets the needs of the global Internet community, should be made under an open and transparent renewal process, for the extension of the award at the end of September 2003. The Department is urged to establish formal consultation with users of the IANA services and to take account of their views when considering a first one year extension in September this year.

### **Doc 57: Niue**

Niue is a small island nation in the South Pacific. It is approximately 120 square Kilometers. Although a place of great natural beauty, due to the natural topography, it has no suitable harbors for cruise vessels. Its primary link to the outside is via air travel, however there are only a few flights per week to the island. It is an independent nation, in free association with New Zealand. Its natural resources are limited and communications are through a leased circuit on a satellite. As a result of these factors, their national budget is exceedingly tight and there is little to spare to fight legal battles. In 1997, the rights of the sovereign county of Niue to participate in the Internet and to control the utilization of their ccTLD, ".nu", were usurped. Niue, as a small developing nation has been unable to have those responsible rectify their actions and return control to the nation. Niue cannot bring legal weight to bear against the ccTLD registry manager as the manager's place of residence is in the United States and his base of operations is primarily in Europe. There is no apparent forum where the actions taken by the US Dept of Commerce and IANA can be made right. Fear of legal action by the manager has made them unwilling to act. WIPO is not a suitable avenue to gain the return of the gov.nu name. Niue is effectively blocked from participation in the Internet, even to communicate with its own citizens at home or abroad.

While Niue fully adheres to and supports the principles utilized by ICANN and established by the GAC for the management of cctLDs, the ccTLD manager has taken every measure possible to avoid the utilization of these concepts, preferring instead to support his claim only through RFC 1591. As such, many of the efforts of the Government have been to show that even under RFC1591, the delegation is flawed and should be re-delegated per the laws and national public policy of Niue.

The paper provides a detailed description of the situation from Niue's point of view.

## **Doc 58: Center for Democracy and Technology**

Each country in the world has been assigned a country code top-level domain name (ccTLD), and for each ccTLD, there is a designated manager. For a number of countries, especially in the developing world, the ccTLD manager is a for-profit entity located outside of the country to which the domain name relates. In such cases, it may be desirable to redelegate management of the ccTLD to a local entity, to bring the management of the ccTLD inside the territory of the country involved and to make the administration of the domain name more responsive to the public interest. This paper outlines a strategy for achieving such a redelegation.

Delegation and redelegation of the management of ccTLDs is controlled by the Internet Assigned Numbers Authority (IANA). The IANA function is performed by the Internet Corporation for Assigned Names and Numbers (ICANN) under a contract with the U.S. Government. Performance of the IANA function includes receiving delegation and redelegation requests concerning ccTLDs, thoroughly investigating the circumstances surrounding such requests, and resolving them.

In acting on redelegation requests, IANA follows the policies and practices summarized in “Internet Domain Name System Structure and Delegation” (ICP-1) and a document known as RFC 1591. Since May 1999, IANA has approved a number of requests for redelegation of ccTLDs, including the Pitcairn Islands (.pn), Canada (.ca), Australia (.au), the United States (.us), and Japan (.jp), after careful investigation and after concluding that there was widespread support in the local Internet community.

Several conclusions can be drawn about ICANN’s approach to redelegation requests: (i) A request should include a detailed description of the proposed registry policies and the technical competency of the new manager. (ii) ICANN appears to disfavor delegations to government agencies, preferring delegations to non-profit entities that represent all interested parties. (iii) ICANN is reluctant to choose among competing relegation requests, preferring to be presented with a proposal that represents consensus within the government and the broader Internet community in the country. The approach most likely to succeed is one based on the creation, with government support, of a private, non-profit entity that would operate the domain space in the interest of the affected nation’s Internet community.

IANA now essentially requires redelegations to be based on three written agreements, known as the triangular arrangement: (1) an agreement between the private, non-profit entity and the government; (2) a communication between the government and ICANN expressing the support of the government as a whole; and (3) an agreement between ICANN and the new manager.

It must be recognized that redelegation may not happen quickly, particularly if the incumbent manager does not consent. ICANN itself is in the midst of major debates about its structure and mission, and will probably be absorbed with its own evolution for some time. Nevertheless, if the government of the affected country and the national Internet community are patient and follow the steps that have led to success in other cases, redelegation is likely to happen.

The paper gives a checklist for redelegation. One of the key steps is:

Develop, in consultation with the government, a private sector, non-profit entity, similar to auDA, which will agree:

- To operate as a fully self-funding and not-for-profit organization;
- To operate the ccTLD for the purpose of fostering development of the national Internet community, as well as the global Internet community;
- To be inclusive of and accountable to all members of the Internet community in the country;

- To adopt open, transparent and consultative processes;
- To not acquire any property rights in the ccTLD itself;
- To enhance benefits to Internet users by promoting competition, fair trading, and consumer protection and providing access to technical support;
- To establish dispute resolution mechanisms that take into account intellectual property, consumer protection and other internationally accepted laws; and
- To abide by ICANN's policies.

Another is:

The government should be prepared to make a communication to ICANN in which it agrees to:

- Recognize ICANN as the appropriate international entity to oversee technical coordination of the Internet in a way that preserves it as an effective and convenient mechanism for global communication;
- Acknowledge respect for the public policy objectives of: transparency and non-discrimination; respect for personal privacy; greater choice, lower prices, better service, and better consumer protection for Internet users; and
- Ensure that the new non-profit operates in conformity with these public policy objectives and international law.

Except in countries lacking Internet, IANA prefers that the manager of a ccTLD be located in the country of the ccTLD, and not abroad, in order to be more responsive to the public interest and subject to national laws. In weighing requests for redelgation, IANA is most likely to act if three conditions are present:

- The redelegation would be to a non-governmental, non-profit entity that broadly represents the national Internet community;
- There is broad and documented support for the new entity across the government and the national Internet community.
- The new entity is backed by a sound technical plan for the registry.

IANA has also considered it important that a new manger (1) embody the principle of private sector self-regulation, with the government playing a supportive but non-intervening role; (2) operate through open, transparent and inclusive processes; and (3) clearly benefit the local Internet community.

---