Unclassified **DSTI/ICCP/TISP(2006)6/FINAL**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

17-Nov-2006

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

Cancels & replaces the same document of 15 November 2006

Working Party on Telecommunication and Information Services Policies

EVOLUTION IN THE MANAGEMENT OF COUNTRY CODE TOP-LEVEL DOMAIN NAMES (ccTLDs)

JT03217988

Document complet disponible sur OLIS dans son format d'origine
Complete document available on OLIS in its original format

FOREWORD

This report was presented to the Working Party on Communication Infrastructures and Services Policy (CISP) in May 2006 and was declassified by the Committee for Information, Computer and Communications Policies (ICCP) in October 2006. This report was prepared by Ms. Karine Perset, with the participation of Mr. Dimitri Ypsilanti, both of the OECD's Directorate for Science, Technology and Industry. This report is published on the responsibility of the Secretary-General of the OECD.

Documenting activity and issues faced by country code top-level domain (ccTLD) operators can benefit those who seek to make policy decisions on related matters. For example, the Governmental Advisory Committee to ICANN (GAC) has identified both ccTLDs and internationalised domain names (IDNs) as key priority areas for early engagement[1] and the GAC has formed a joint task force on ccTLD matters with ICANN's country code Names Supporting Organisation (ccNSO).

This paper aims to provide a general overview of country code top-level domains (ccTLDs) across the OECD area as well as in other areas that are experiencing high growth in the use of ccTLDs in terms of *i)* quantification of registrations and demand trends; *ii)* trends in the administration of ccTLDs; *iii)* current and ongoing policy and technical issues faced by ccTLD managers such as internationalised domain names (IDNs), Whois, or security, and finally; *iv)* ccTLD managers' institutional relationships with each other, with governments, and with the Internet Corporation for Assigned Names and Numbers (ICANN).

This document builds on the content of earlier documents, which include OECD, 2006, "The Secondary Market for Domain Names", OECD, 2005, "OECD Input to the United Nations Working Group on Internet Governance (WGIG)", OECD, 2004, "Generic Top Level Domain Names: Market Development and Allocation Issues", OECD, 2003, "Comparing domain name administration in OECD countries" and OECD, 1997, "Internet Domain Name Allocation Policies".

TABLE OF CONTENTS

INTRODUCTION

The number of domain names is growing faster than at any time, reaching over 93 million registered domain names in April 2006.[2] One reason for this is the continued expansion of the World Wide Web with some 80 million websites in operation by April 2006.[3]

The domain name system (DNS) was conceived as a scalable distributed mechanism to resolve user-friendly host names (*e.g.* www.oecd.org) into a numeric Internet (IP) address (*e.g.* 203.160.185.48). Hierarchical DNS names are supported by the "dot" in the name, and structured from right to left. The data in the DNS is stored in hierarchical and widely distributed sets of machines known as "name servers", which are queried by "resolvers".[4] Invisible to users, the top of the hierarchy is the "root", and the root servers that mirror this root. Root servers replicate the root, and provide information enabling resolvers to find details of the level below, known as the Top-Level Domain (TLD). The TLD is the last label on the right hand-side of the domain name (.org, .com, .jp or .fr). For example, a domain name used by the OECD is "oecd.org" and ".org" is the TLD. The next level of the DNS is called the Second-Level Domain name (SLD) (*e.g.* "oecd" in "oecd.org").

The TLDs are divided into two classes, one of which is that of generic Top-Level Domains (gTLDs) (*e.g.* ".com" or ".org") and the other of country code Top-Level Domains (ccTLDs). A country code top-level domain (ccTLD) is a top-level domain used and reserved for a country or an dependent territory, expressed in two-letter country codes mostly based on the ISO 3166-1 standard (*e.g.* ".au" for Australia or ".fr" for France), although there are several exceptions.[5] In many countries, extensive use is made of the country's top-level domain. In other countries, most domain name registrations are under gTLDs rather than the local ccTLD.[6] The country's top-level domain represents the national or territorial interests of a domain, and is often viewed as the flagship of a country's Internet participation and as a strategic asset with symbolic, socio-economic and/or Internet stability and security implications.[7]

The number of domain name registrations under major gTLDs and the ccTLDs has increased rapidly over recent years. The major gTLDs more than doubled from 28 million in 2000 to 60 million in 2005, while the number of registrations in the ccTLDs nearly tripled from 12 million in 2000 to 33 million in 2005.

Whereas gTLDs do not generally have geographic or country designations and are governed by rules set up by the Internet Corporation for Assigned Names and Numbers (ICANN)[8], ccTLDs, for their part, are under national jurisdiction for the definition of their policies and legal responsibilities.[9] This local responsibility has been made clear in the Principles and Guidelines for the delegation and administration of ccTLDs suggested by the Governmental Advisory Committee (GAC) of ICANN.[10] Country code Internet domain names, beyond being addresses, often serve as roadmaps to national Internet identities and priorities, as reflected in the ICANN GAC Principles and Guidelines document.

In the DNS context, there are three main actors. CcTLD "registries" are commonly understood as entities that are responsible for administering and operating a ccTLD in compliance with local and/or regional legislation and relevant agreements. In many cases, registry-accredited "registrars", or domain name retailers, purchase domain names from ccTLD registries on behalf of registrants and in accordance with the specific ccTLD policies as specified in registrar accreditation agreements, and provide services to registrants. Finally, "registrants" or "domain name holders" are individual or reseller customers of the registrar or of the registry.

MAIN POINTS

There is high growth in ccTLD domain name markets

Attention should be given to the uniqueness of ccTLD names and the associated responsibility of the ccTLD registries. Overall, countries have become more aware of the importance of the Internet and of Internet identifiers, and many ccTLD registries strive to enhance their national Internet identity by promoting registrations under their ccTLD. Reduced restrictions on registration requirements, commercialisation and greater automation of registry provisioning have accelerated adoption of ccTLD names. Yearly growth in registrations under ccTLD averaged 36% in 2005. Some of the higher growth rates are found in countries that have liberalised their registration requirements (*e.g.* China, Brazil, and India). Meanwhile, OECD country ccTLDs experienced a lower growth of 9% and their share of the global ccTLD market has gone down from 90% in 2004 to 79% in 2005, as a result of the faster growth in non-OECD markets.

The take-up of ccTLDs varies widely and the trend is towards liberalisation of the ccTLD name space

There are very large differences in the take-up of ccTLD names across countries, depending on the historical policies applied to registration: registrations under the top-10 ccTLDs represented 60% of the global ccTLD market in 2005, and the German and UK registries alone represented over 50% of ccTLD names registered. Registrations under ccTLDs represent 35% of top-level domain registrations, a proportion that has overall slightly increased over the past five years. An attribute of widely used ccTLDs is that they tend to encourage a registry-registrar-registrant model whereby the ccTLD registry's distribution network is large and hence they tend to benefit from economies of scale that they are able to pass on to registrars and registrants in their pricing policies. Differing growth rates between country code registries are largely a result of the goals of the registries, which may place more or less restrictions on registrations and set prices at different levels.

Rules for registration of ccTLDs are largely being liberalised and options widened through the use of registrations as third-level domain names (*e.g.* example.co.uk) because, while ccTLDs might be local, alternatives are global. Even though most ccTLDs managers are not-for-profit, they may benefit from economies of scale from registering large quantities of ccTLD domain names and as mentioned previously, a further incentive to put forward ccTLD domain names is that they are often viewed as flagships of a country's Internet participation. Some ccTLD registries – such as in Austria (at) and the Cocos Islands (cc) – allow anyone to acquire a domain in their ccTLD regardless of trademark, trade name or location, while others allow only local entities or entities with a trademark to acquire a name in their ccTLD. Many registries differentiate requirements according to the meaning of a second-level domain.

There are pros and cons to liberalising requirements for registering a domain name. While registry requirements such as a local presence or trademarks for businesses may raise the threshold in terms of cost and administrative processes necessary to register a domain name[11], some have found that such requirements can help contribute to curbing cyber-squatting, online fraud and intellectual property violations and help provide assurance to consumers and companies that they are dealing with legitimate locally-based entities.

ccTLD registries are mostly not-for-profit organisations that aim to be responsive to their local Internet communities

A large number of ccTLD managers are local organisations that are not-for-profit organisations with a public service inclination. They tend to emphasise an active commitment to the needs of their local Internet communities (LIC), in compliance with local and/or regional legislation, while forming part of and taking into account a global inter-dependent system. The composition of given "local Internet communities" varies from one country to another, and might include Internet service providers, Internet users – both individual and business –, as well as governments. Therefore the form, characteristics and influence of the LIC on domain allocation vary significantly.

CcTLDs are responsible to the Global Internet Community for interoperability with the global Internet through relationships with, *inter alia*, ICANN, Regional Internet Registries, other TLDs, or the Internet Engineering Task Force. While different ccTLD domain names carry different meanings and are usually not perfect substitutes, on the global Internet if users do not believe their ccTLD to be their best alternative they can and do register names under other top-level domains – a necessary incentive for ccTLD registries to be commercially competitive and attractive locally.

Furthermore, the apparently simple distinction between country code Top-Level Domains (ccTLDs) and generic Top-Level Domains (gTLDs) (*e.g.* ".com" or ".org") is actually more complex, as the differences among TLDs do not only relate to whether they were originally associated with a country code or a generic category, but rather to the policies that they operate under. Some ccTLDs, often referred to as "open ccTLDs", act as commercial gTLDs. "Open ccTLD" registries are not subject to the rules for gTLDs that the ICANN community develops but in most cases are subject to regulations of the country or the region in which they are based.[12]

Government interest and involvement in the management of their national ccTLD has increased, though not necessarily to increase control

The Tunis Agenda (the second phase of the World Summit on the Information Society in 2005, paragraph 63) recognised that governments have legitimate interests in the management of their respective ccTLD, which should be respected. Many parties have acknowledged that ccTLDs are managed in the interest of the local community and in compliance with local and/or regional legislation. Yet a question often raised is whether or how to implement authority of governments over their ccTLDs within current frameworks in a way that is suitably dynamic in serving the interests of national and international registrants and to that question, there is no "one size fits all" solution.

Best practice includes deciding whether to formalise the relationship between governments and ccTLD managers, through a letter of acknowledgement, a contract, and/or legislation that determines how public policy authority is exercised.[13] In some contexts, legislation and/or a formal agreement between governments and ccTLD managers may be in the national interest. However, some deem that such agreements might be of little practical use because many ccTLD registries and domain registrations under each ccTLD (even where the ccTLD registry itself is based in country), depend on an underlying (name server) infrastructure that is neither based within their country nor within the sphere of national government control and that, in addition, public procurement rules might involve undesirable time delays.

CcTLDs have a variety of policies depending on national cultural, economic and legal circumstances

The ccTLDs have a wide variety of naming structures. In April 2006 there were 245 country code top-level domains (ccTLDs), such as .jp or .nl, compared with 19 generic top-level domains (gTLDs). The

TLDs are the top level of the naming hierarchy. The ccTLDs have a particularly wide range of structures, from flat to multi-layered, some having several levels of hierarchy and elaborate structures, which may be structured with generic or geographic second-level domains such as example.la.ca.us or example.co.jp, and others having flat structures with many second-level names, such as example.de.

Most ccTLD registries have their own policies with regards to eligibility for registrations, local presence requirements, naming structure of the second-level domains, public access to ccTLD registration information (Whois), and trademark policy, that are both heavily influenced by, as well as subject to, local or regional legislation. Many feel that such variety is in the interest of registrants as it allows each registry to reflect local requirements, and that the variety of approaches is a strength of the ccTLD community, facilitating the identification of best practice and cultural diversity.

ICANN's country code Name Supporting Organization (ccNSO) was created to propose best practices and global policies, for example best practices for technical issues. Although increased best practices may be in the interest of registrars and registrants, at this stage it remains unclear to some ccTLD managers which policy areas will benefit from global, as opposed to regional or local, best practices and policy development by the ccNSO.

For the ccTLDs managers and the ccNSO, both DNSSec (short for DNS Security Extensions) and Whois have been ongoing topics of debate. A set of standards for securing the DNS data, DNSSec-bis, is in the process of being implemented and is expected to considerably increase the security of DNS servers.[14] Solutions for known privacy problems ("zone walking") are still under development.[15]

Whois is a protocol to query a registry's database for information about domain name registrations. Public access to accurate Whois data provided by both ccTLDs and gTLDs involves a range of public policy issues, and Whois-type databases must necessarily be in conformity with national law on data protection and privacy, which vary across countries, preventing the establishment of a universal Whois data provision and access policy across ccTLDs and gTLDs. Many ccTLD registries have implemented technical solutions to prevent Whois abuses. An on-going policy development process on Whois by ICANN's generic Name Supporting Organization has provided the impetus for renewed focus on Whois by the GAC, which is considering principles that could be utilised to balance privacy and law enforcement/consumer protection interests.

Large ccTLDs registries with many accredited registrars are also seeing the types of behaviour that have characterised large gTLD registries and which some qualify as "gaming the system" by directly registering domain names for resale at a premium and/or exploitation. In some cases, when registrars have direct access to the registry databases, they query ccTLD databases in order to determine which domain names are close to expiration and will soon be deleted from the registry, in cases where the contractual relationship between the domain holder and registry has a finite length. The intent is to seize the names as soon as they expire by pooling together as many registrar accreditations as possible when each registrar has equivalent access to registries. Their reason is often that these domains might have "monetisation" potential: domain names are used to help attract traffic from search-engines and generate cost-per-click advertising revenue. In other cases, registrars will also pool together as many registry accreditations as possible to register valuable names when new TLDs or new SLDs are introduced.

Internationalised domain names (IDNs) are a pressing priority for many countries and Internet communities: government initiatives are called for to help educate end-users and build awareness

Efforts to support internationalised domain names, e-mail addresses, keyword lookup, as well as multilingual content, are four distinct and complementary priority areas in which improvements would facilitate some language populations benefiting from the Internet. Internationalised domain names (IDN), *i.e.* supporting Unicode characters in domain names, are a priority for many countries in the world. The demand for IDN is based on the desire to increase access to the Internet for people who do not use or recognise Latin characters and on the related wish for Internet identifiers to reflect cultural variety. Efforts to support access to the Internet through IDN and to co-ordinate work across different countries, regions, and language groups are welcome and ongoing. A number of governments or public authorities are involved in promoting IDNs and many registries have already adapted the standard to support IDN registrations at the technical level. Actual use is being impeded by the fact that consumers may need to update their local application software to ensure end-to-end IDN communication. Hence there is a clear role for governments to play in educating Internet users and building awareness of the necessary client-side application updates.

Deployment of IDNs at the top-level raises complex policy questions, underscoring the necessary co-operation of all stakeholders.

The issue today is to put in place processes for development, maintenance, upgrade and IDN resolution in applications that use uniform syntax/semantics in all applications. A number of challenges, including language issues, technical and security issues, commercial availability of client software, and concerns about fragmentation of the global name space, are under consideration by groups such as ICANN or the ITU, to enable full deployment of internationalised domain names.[16] Since the end of 2005, ICANN has fully taken on the issue of IDNs. A joint working group comprised of ICANN’s generic Names Supporting Organization (gNSO) and country codes Names Supporting Organisation (ccNSO) was set up to issue a paper discussing the associated policy issues that need to be dealt with before introducing IDNs at the top-level domain. The gNSO issued a preliminary issues report in May 2006, listing wide-ranging policy issues that include competition in ccTLD markets and gTLD markets, consumer protection, methods for selection and allocation of IDN TLDs, and intellectual property rights. [17]

Meanwhile, technical tests of two approaches to the insertion of IDN at the TLD are being developed within the ICANN President Advisory Committee that has been established to discuss key IDN implementation issues. [18]

Although ccTLD managers are increasingly entering into agreements with ICANN, some continue to choose not to do so

Although a majority of ccTLDs lack a formal agreement with ICANN, some ccTLDs have entered into or are in the process of formalising their relationship with ICANN. They do this by entering into “Accountability Frameworks”, which list the set of responsibilities of both the ccTLD and ICANN[19] or by a less formal “exchange of letters” whereby each party recognises its respective responsibilities. In parallel, some ccTLDs are becoming members of ICANN’s ccNSO, which is an independent process that entails developing policies which are binding for ccNSO members within the limits of national law. The ccNSO was created in 2002 to give a voice to ccTLD registries within ICANN processes, and to enable ICANN in performance of the IANA functions to be able to give better support to ccTLD managers. It is a policy-development body responsible for *i)* developing and recommending to the Board global policies relating to country-code top-level domains; *ii)* nurturing consensus across the ccNSO's community, including the name-related activities of ccTLDs; and *iii)* co-ordinating with other ICANN Supporting Organizations, committees, and constituencies under ICANN. CcTLD registries communicate and co-operate with ICANN when they request changes through the IANA services. Beyond the IANA functions, possible themes within the ccNSO might include policy on deployment of IDNs at the top-level and preserving universal resolvability, as well as outreach.

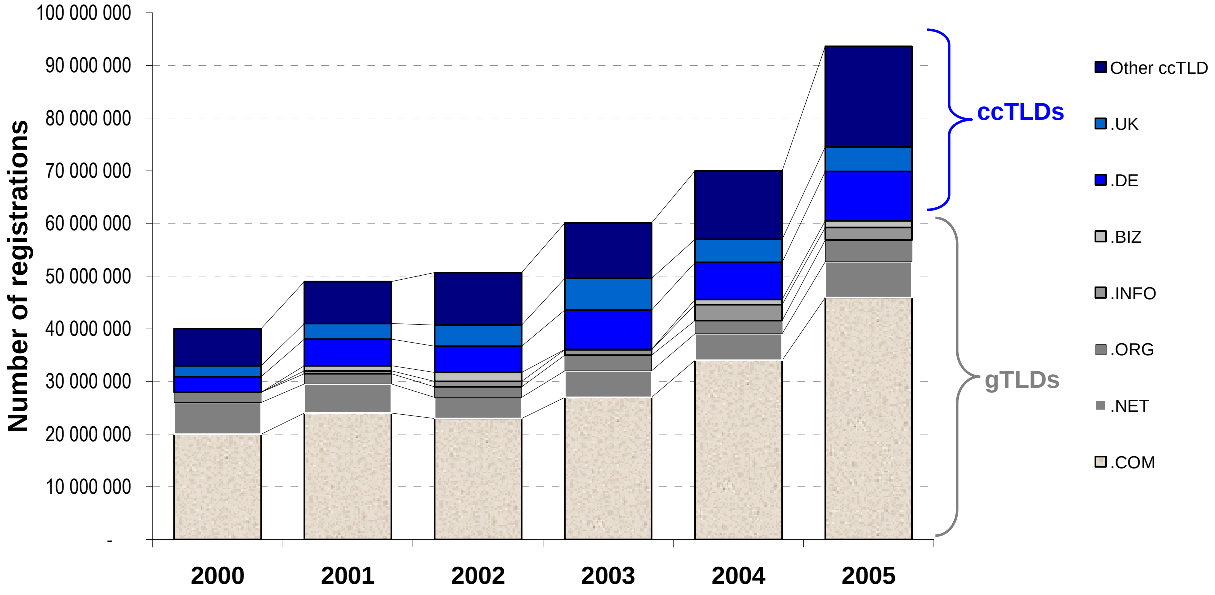
QUANTIFICATION OF CCTLDS

Number of registrations and growth rates

The number of domain name registrations under both major gTLDs and the ccTLDs has increased rapidly over recent years. From over 60 million in 2003, the number of top-level domain names reached over 70 million by the end of 2004 and over 93 million by the end of 2005.

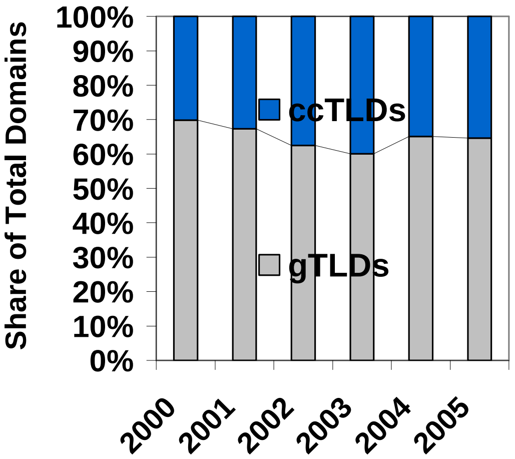
Registrations for the major gTLDs more than doubled from 28 million in 2000 to 60 million in 2005 **(**Figure 1**)**, while the number of registrations in the ccTLDs almost tripled from 12 million in 2000 to 33 million in 2005.

Figure 1. Number of registered gTLDs and ccTLDs, 2000-2005



Source: Based on ZookNIC (www.zooknic.com) and VeriSign (2006).

Figure 2. Registrations of gTLDs and ccTLDs, 2000-2005



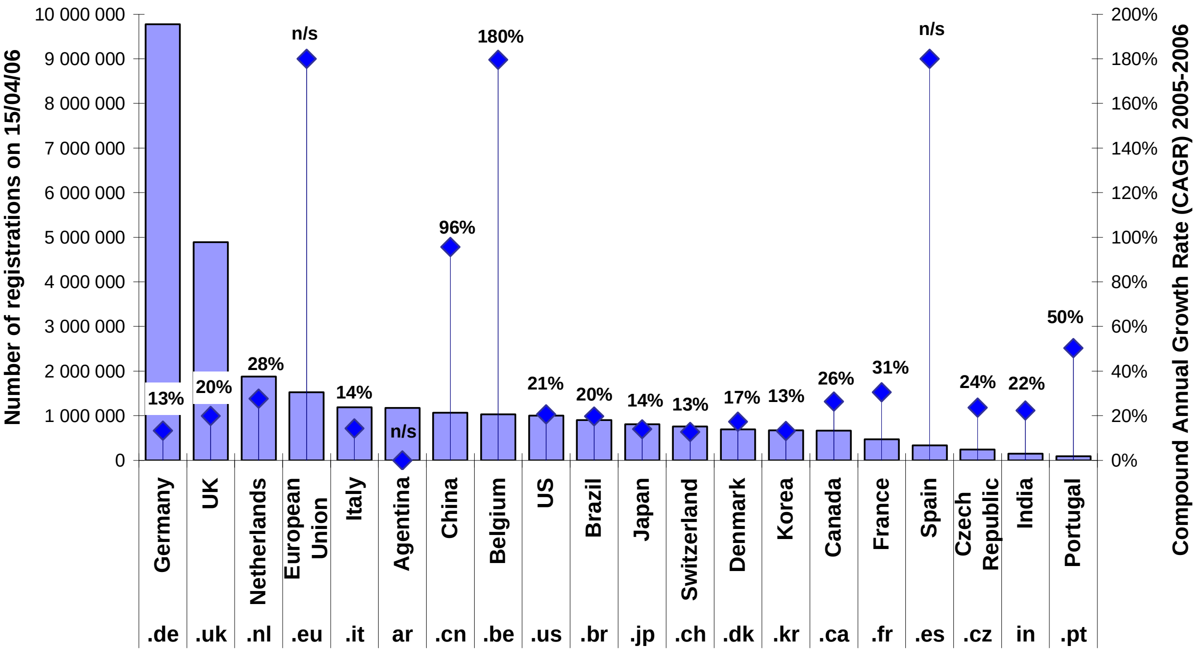
Source: Based on ZookNIC (www.zooknic.com) and VeriSign (2006).

Over the past five years, ccTLDs registrations have increased as a share of total domain name registrations (Figure 2**)**. Accounting for 30% of registrations in 2000, they accounted for about 40% in 2003 and 35% of registrations in 2005.

Differing growth rates between country code registries are largely a result of the goals of the registries, which may place more or less restrictions on registrations and prices may vary. It is believed that, for instance, the large adoption of the German country code TLD, with close to 10 million names registered in .de, is due to a combination of factors. These include policies by the registry that have been largely unrestricted since the early days, a strong level of Internet use in Germany and comparatively low prices. .de's marked adoption and recognition in Germany is clear in that it has 90% of the total domain name market in Germany and little registrations from outside Germany. Other registries, such as the registry for Jordan (.jo) place very strict rules on trademarks: hence there might be only be a very low level of registration activity. It can be argued that if a national registry places very restrictive conditions on registrations, it increases administrative burden and associated cost and pushes local users to shift their registrations offshore. On the other hand, registration requirements for specific entities, such as trading entities, may help foster end-user trust. In this regard, the widespread use of registrations under second-level domains – such as .co.jp or .gouv.fr – may help to differentiate requirements based on the registering entity.

Much of the growth in ccTLD registrations is coming from developing nations, from ccTLD registries that are liberalising their policies, and from specific promotional campaigns. For example, the number of domain names using China's .cn more than doubled in 2005, according to ZookNIC.[20] The reasons for this include higher growth in Internet usage, a major lowering of the price of registration, and implementation of Chinese character domain name registrations at the second level.

Figure 3. Top 20 ccTLD registries in terms of number of registrations in April 2006 and CAGR over 9 month period from June 2005 to April 2006

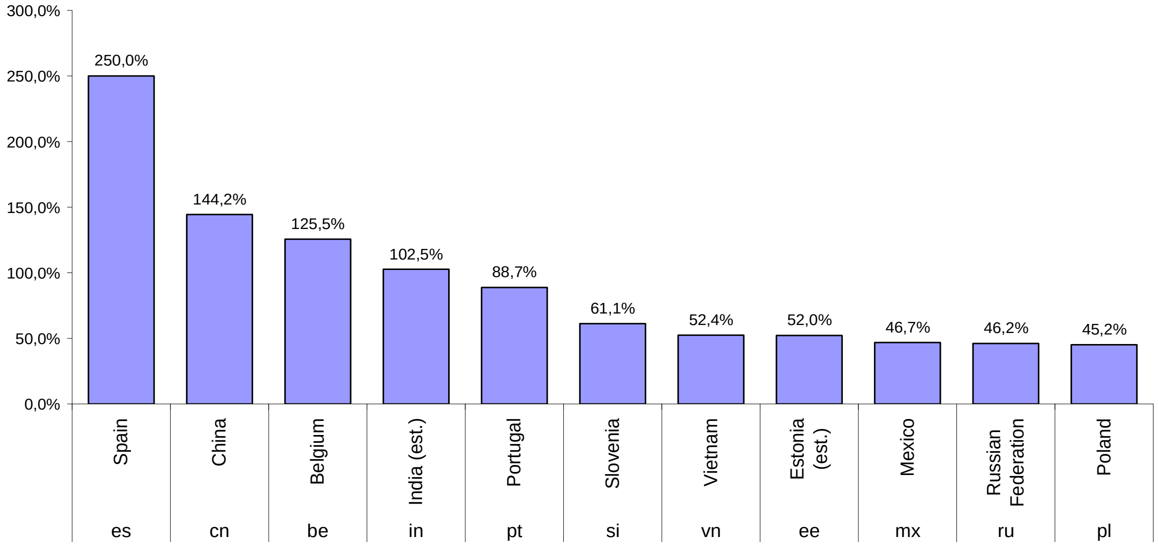


Source: Registry counts 2006 and ZookNIC, June 2005.

The vast majority of ccTLD registrations are attributable to a relatively small number of ccTLD registries. Out of the 245 ccTLDs, the top ten account for 70% of all ccTLD registrations and nearly all of the top ten ccTLDs experienced growth from mid 2005 to April 2006. .eu entered the scene very quickly, .be benefited from a free 3-month promotional offer, and .cn (China) experienced sustained high growth **(**Figure 3**)**.

While the top-ten ccTLDs represent a large proportion of the total number of ccTLD registrations, this percentage has been slowly declining since early 2004 when the top ten represented 75% of all ccTLDs. The gradual change reflects the high growth (Figure 4 shows the highest growth rates in 2005) in some previously small(er) ccTLD registries, including some experiencing double-digit or triple-digit growth such as .in (India), .ru (Russia), .pt (Portugal), .mx (Mexico) or .es (Spain).[21] The overall ccTLD domain name base experienced 5% quarter-over-quarter growth and 21.5% yearly growth. The largest ccTLD continues to be .de (Germany) in terms of the total base of domain name registrations with .uk (United Kingdom) as the second largest. Together, .de and .uk represent 43% of the ccTLD base with an average yearly growth of 13% and 20% respectively. Nominet, the not-for-profit company that administers all registrations of the .uk suffix, has a very liberal registration policy. In contrast with other ccTLDs, .ar registrations handled by NIC-Argentina are still free of charge, which has encouraged a large number of registrations. However, domain name renewal fees are planned in the future.

Figure 4. Highest ccTLD growth rates in 2005



Source: ZookNIC, 2006.

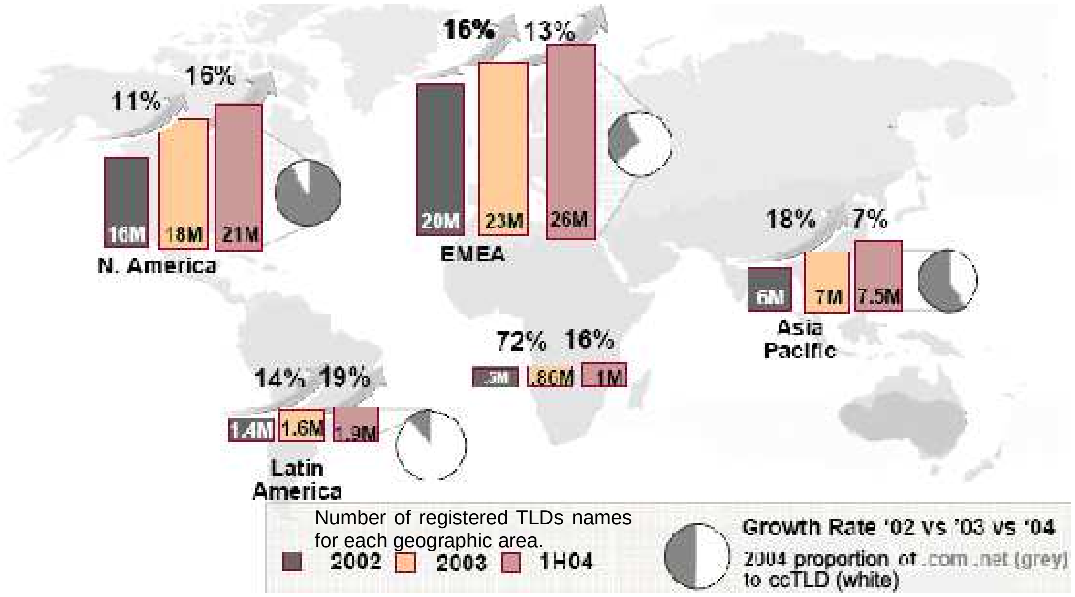
Box 1. DNS BE, the ".be" registry, has seen a spectacular increase in recent months

The increase of registrations under .be is the result of a promotional campaign that ran for three months, from November 2005 through January 2006. The DNS BE registry offered over 500 000 free .be domain names to registrars who in turn often chose not to charge registrants for new names. Accompanied by a large advertising campaign[22], the goal was to stimulate interest by private end-users in registering a .be domain name. In just three months[23], the number of .be names went well over the 1 million mark - more than doubling the previous total. The objective of the advertising campaign was to show individuals how easy it was to have their own Internet identity. Since DNS BE works along the lines of the Registry-Registrar-Registrant model with no direct registrations, the purpose of advertising was to create awareness and support the registrars in their commercial activities.

Domain name registrations by region

In Latin America and to a lesser extent in Europe, ccTLDs constitute a majority of the TLDs registered. In contrast, in North America and to a lesser extent in the Asia Pacific region, ccTLDs are a minority of the TLDs registered (Figure 5 shows the proportion of ccTLDs (white) versus the proportion of gTLD .net/.com (grey) top-level domains in 2004). This can largely be attributed to historical facts and the early and continuing adoption and popularity of gTLDs in the United States. Of further interest, while 76% of registered ccTLDs were European in 2004, large growth rates are currently being experienced in Latin America, the Middle East and Africa, and in the Asia Pacific region.

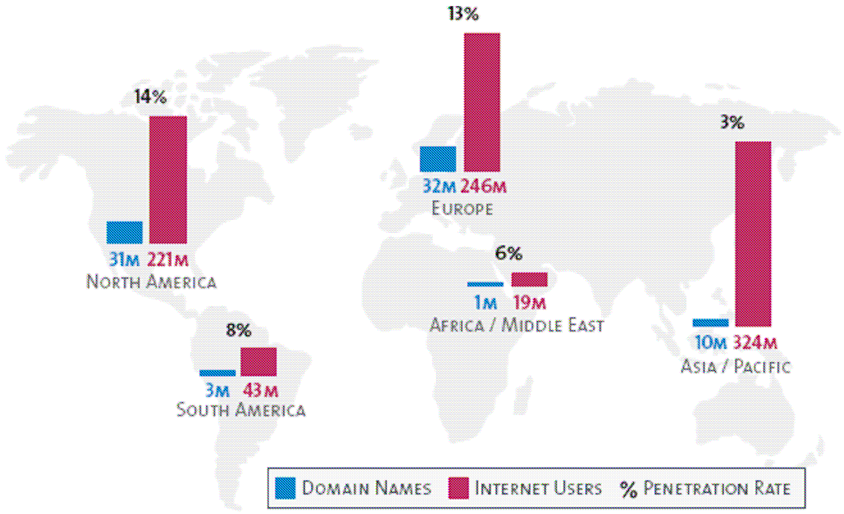
Figure 5. Geographic distribution of ccTLDs and selected gTLDs (.com and .net)



Source: Zooknic, Inc., July 2004.

As shown in Figure 6, the Asia Pacific and Africa and Middle East regions had a disproportionately low stock of registered domain names relative to the number of Internet users in July 2005 (on average respectively 3 and of 5% of Internet users owned a domain name) compared to North America and Europe (where respectively 14% and 13% of Internet users owned a domain name).

Figure 6. Domain Name Registrations by Geography, July 2005

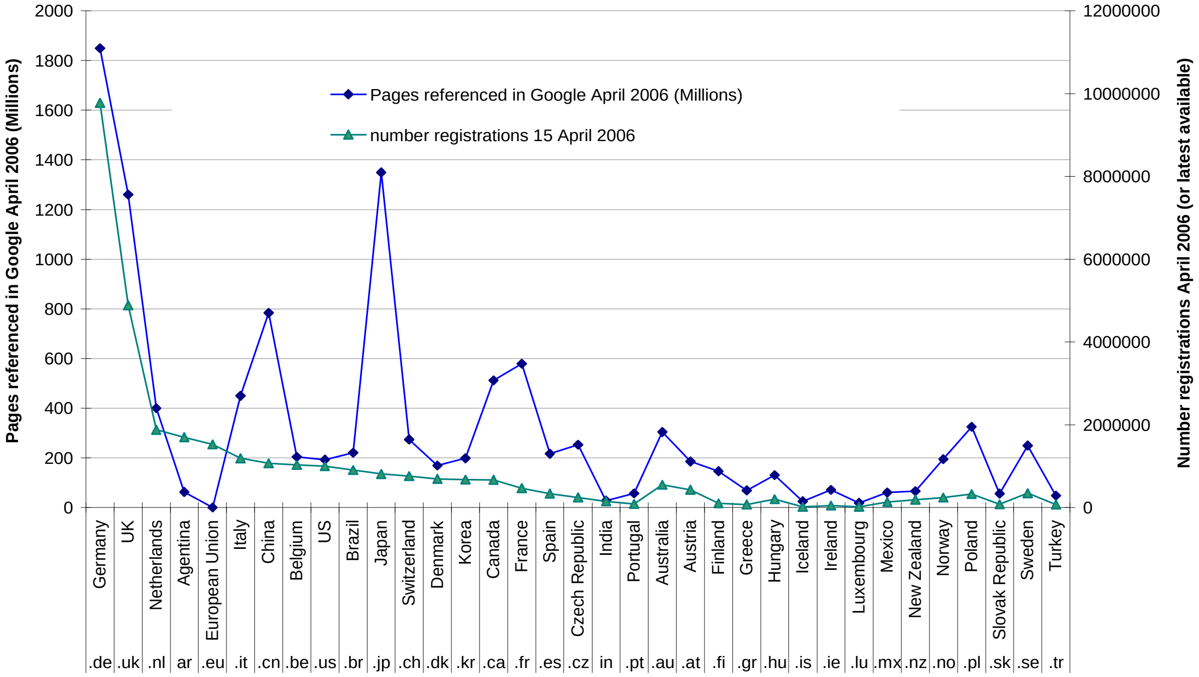


Sources: VeriSign 2005; Zooknic, July 2005; ClickZ Stats, July 2005.

Search engine visibility by TLD

If a search-engine such as Google references most web content, these results would give an indication of the amount of content in each TLD; if Google indexes roughly the same proportion of content within each TLD (*i.e.* indexes about half of .uk and about half of .cc), then comparison of Google page counts provides an approximation of the relative sizes of TLDs in terms of pages named under that TLD.

Figure 7. Search engine visibility by TLD



Source: OECD, 2006.

Figure 7 summarises Google indexes of TLDs for comparison. In many cases, the number of pages referenced by Google seems to be in line with the number of domain name registrations. There are significant outliers, of which some can be explained by the registration policies or by the date of launch of the TLD. For instance, .eu's lack of search engine visibility can be explained by the fact that the TLD had only recently opened and hence web sites were yet to be built and referenced by the search-engine.

Search-engine queries typically use domain names, both top-level and secondary, as one of the criteria for gauging the relevancy of a page for a given query. This influences some users to register under ccTLDs as well as gTLDs. Information search technology, through web-based indexing and search systems such as Google and Yahoo, is producing increasingly relevant results and considerably facilitating the way in which information and services are accessed. In an Internet search, the user uses a query language to describe the nature of documents, and in response, a search engine locates the documents or other types of digital files that "best match" the description. Search engines may use domains as one of the criteria for local search results. For example, a search on google.com.au for “pages from Australia” may only return web page results that are under .au or of which the IP (Internet Protocol) address is assigned to an Australian autonomous system number (ASN). This influences some users to register under ccTLDs as well as gTLDs in order to get picked up locally by a search-engine. There might also be other practical side impacts for e-business related to fraud protection. For instance, PayPal has been reported not to work for an Australian e-business site without an .a e-mail address.

TRENDS IN THE ADMINISTRATION OF COUNTRY CODE TOP-LEVEL DOMAIN NAMES POLICIES

ccTLDs as Internet identities

At present, there are 245 ccTLDs[24] in the world and each ccTLD is administered by its ccTLD registry who is “a trustee for the delegated ccTLD, and has a duty to serve the local Internet community as well as the global Internet community”.[25] As the Internet developed and as countries became more aware of the importance of the Internet, an increasing number of governments became interested in the oversight or management of their country code top-level domains.[26] Government involvement in ccTLDs has sometimes been about establishing a legal basis for ccTLDs or determining who has national authority. In some cases, ccTLDs are subject to an agreement/contract with a government or legislation and oversight mechanisms, or are government-run. In other cases, the relationship between ccTLDs and governments is very informal, such as in the cases of the German .de and the British .uk. As the Internet has increased in importance governments have increasingly viewed country code domain names as a strategic part of their Internet policy, part of their national sovereignty, and in some cases, as a source of revenue.

Conceived in the early 1980s by Jon Postel, a computer scientist at the University of Southern California, to help organise Internet addressing by using the two-letter codes from the ISO 3166 list of countries, country code domain names were not originally intended to be official. Until the late 1990s the sole requirements to operate a ccTLD were for the administrative contact for each country code to reside in the given country and understand they were "performing a public service on behalf of the Internet community".[27] Thus some country code registries are operated on the basis of a historical/legacy assignment by IANA, by volunteers, through agreement with ICANN and sometimes the associated government.

Partly due to choice, partly due to legacy situations, ccTLD registries have various statuses depending on the country.[28] A review of the ccTLD registries in OECD member countries and several countries in which ccTLD registrations are fast-growing, shows that a majority are not-for-profit organisations, which are often called Network Information Centers (NIC), formed by ISPs and Internet related organisations, and in which governments might have a role. In Germany, Denic is a co-operative, the members of which are profit-oriented companies. Other registries define themselves as “private companies”, such as JPRS in Japan, Nominet in the United Kingdom, or Neustar in the United States, although there is a significant difference between a private operation that is membership-driven, such as Nominet (.uk) and companies that are running the registry under contract, such as Neustar (.us) under contract with the United States Department of Commerce agency National Telecommunications and Information Administration (NTIA).[29] Other registries such as those of Spain, Korea or Argentina are administered by government organisations. A smaller portion of registries, such as those of Mexico, Switzerland and Turkey, are part of academic networks. Yet another, that of Greece, is a “foundation”.

In most cases, national bodies have significant influence over the operations of their national country code top-level domains (ccTLDs), which may or may not be commercially operated. A number of ccTLDs are overseen by their national governments; some have established non-governmental bodies to represent the local Internet community and exercise varying degrees of oversight; some are completely autonomous not-for-profit bodies that operate voluntarily to meet local Internet community interests; others are commercial bodies with some contractual linkage to the national government. In June 2005, the United States NTIA released the "US Statement of Principles on the Internet's Domain Name and Addressing System" which stated "Governments have legitimate interest in the management of their country code top-level domains (ccTLD)". [30] The Tunis Agenda, which was an outcome of the second phase of the World Summit on the Information Society in 2005, recognised that governments have legitimate interests in the management of their respective ccTLD, which should be respected. Paragraph 63 states:

> "Countries should not be involved in decisions regarding another country's country-code Top-Level Domain (ccTLD). Their legitimate interests, as expressed and defined by each country, in diverse ways, regarding decisions affecting their ccTLDs, need to be respected, upheld and addressed via a flexible and improved framework and mechanisms."

In 2005, the GAC issued a revised set of "Principles and Guidelines for the Delegation and Administration of Country Code Top-Level Domains" whereby Guideline 4.2.1. is that "The relevant government or public authority is strongly encouraged to ensure that the ccTLD is being administered in the public interest, within the framework of its national public policy and relevant laws and regulations."[31] The GAC principles and guidelines do not specify how to ensure that the ccTLD is operated in the public interest. The U.K. approach for example is to rely on existing laws and industry self-regulation.

Therefore a question that is raised is that of whether or how to implement governments' authority over their ccTLDs within the current frameworks of national public policy and relevant laws and regulations, while maintaining suitable dynamism to serve the interests of national and international registrants. Best practices include deciding whether to formalise the relationship between governments and ccTLD managers, through a letter of acknowledgement, a contract, and/or legislation that determines how public policy authority is exercised. Some believe that formal agreements between governments and ccTLD managers can be in the national interest. Others believe that formal agreements may be of little practical value because many ccTLD registry databases and domain registrations under each ccTLD (even where the ccTLD registry itself is based in country), depend on an underlying (name server) infrastructure that is neither based within their country nor within the sphere of national government control and that, in addition, public procurement rules might involve unacceptable time delays.

Examples of recent evolution

Many countries are making it easier for users to register names under their ccTLDs, to facilitate these becoming widespread. Their ambition is generally for their ccTLD to become or to remain the logical first choice for all users with connections to a specific country and to give more users the opportunity to register a ccTLD address. In order to do this, they have generally simplified processes, regulations and allotments while maintaining protection for intellectual property rights. The fact that many prerequisites were requested for obtaining some domain names such as .it, .fr, .se, .es or .in contributed to keeping these domains in little use, with many nationals worldwide preferring to register the names in .com. France broadened the right of identifiable companies to purchase domain names in May 2004[32] and saw a growth rate of nearly 88% in the following 12 months. The second phase of the .fr liberalisation involved allowing individuals who have an address in France to register third-level ccTLD domain names, and generated 130 000 additional domain name registrations within the 3 months following the opening to individuals in June 2006, *i.e.* growth of 26% in the total number of domain names registered under .fr. Spain liberalised its ccTLD .es at the end of 2004 and saw growth of 250% in 2005. India liberalised the policies to register a name in .in and chose a new contractor to provide registry services: registered names went from 6 430 in June 2004 to 131 646 in June 2005 – *i.e.* a growth of nearly 2 000%. China has begun to allow foreign companies to register domains under its country code top-level domain, (ccTLD) .cn. The Chinese name space went from restrictive rules to its current more open policies, and .cn plays a central role in China’s economic ambitions. CNNIC is also allowing easier registration via foreign registrars who may market the domain to new markets.

Whether ccTLDs are considered as national assets or not depends on the country concerned. Over a dozen governments or quasi-government organisations have gained control of their country-code domain names in recent years. Usually the names have been acquired from individuals managing them since the 1990s. For example, the Cayman Islands obtained control of its domain name, .ky, from a United States based entrepreneur who was marketing the name in Kentucky. The governments of Kazakhstan and South Africa have also acted to have ICANN re-delegate the domain names associated with their ISO code to a government nominated entity. Many countries are passing or have passed laws to establish a legal basis for their participation in the ccTLDs associated with their country, such as India or France in 2004.

Table 1. Status of ccTLD registry and relationship with government in OECD and selected countries

cc	Country	ccTLD registries	Status[1]	Government Relationship[2]	Government Activity	ccNSO membership[3]	URL
.au	Australia	auDA	Not-for-profit corporation	Formal	Endorsement	Yes	http://www.auda.org.au
.at	Austria	Nic.at	Not-for-profit corporation	Informal	Observer	No	http://www.nic.at
.be	Belgium	dns.be	Not-for-profit corporation	Informal	none	No	http://www.dns.be
.ca	Canada	CIRA	Not-for-profit corporation	Formal	Agreement	Yes	http://www.cira.ca/
.cz	Czech Republic	CZ.NIC	Not-for-profit corporation	Formal	Management	Yes	http://www.nic.cz
.dk	Denmark	DK Hostmaster	Not-for-profit corporation	Formal	Legislation	No	http://www.dk-hostmaster.dk
.eu	European Union	eurID	Not-for-profit corporation	Formal	Legislation[33]	No	http://www.eurid.eu
.fi	Finland	Ficora	Part of government	Formal	Legislation	No	http://www.ficora.fi
.fr	France	AFNIC	Not-for-profit corporation	Formalising	Council reps	Yes	http://www.nic.fr
.de	Germany	DENIC eG	Not-for-profit cooperative	Informal	Observer	No	http://www.denic.de
.gr	Greece	FORTH-ICS	Foundation	Formal	Legislation-Contract with NRA	No	https://grweb.ics.forth.gr
.hu	Hungary	Domain.hu		Formal	Legislation	No	http://www.nic.hu
.is	Iceland	ISNIC	Private sector	Informal	None	No	http://www.isnic.is
.ie	Ireland	IEDR	Not-for-profit corporation	none	Legislation	No	http://www.iedr.ie
.it	Italy	NIC.IT	Not-for-profit corporation	Formal	Management	No	http://www.nic.it/
.jp	Japan	JPRS	Private sector	Formal	Endorsement	Yes	http://jprs.co.jp
.kr	Korea	NIDA	Part of government	Formal	Approval	Yes	http://www.nic.or.kr
.lu	Luxembourg	RESTENA Foundation	Academia			No	http://www.dns.lu
.mx	Mexico	NIC-Mexico	Academia	Informal	Proposed legislation	Yes	http://www.nic.mx
.nl	Netherlands	SIDN	Not-for-profit corporation	Joint project	Cabinet Review	Yes	http://www.sidn.nl
.nz	New Zealand	InternetNZ	Not-for-profit corporation	Informal	Endorsement	Yes	http://www.domainz.net.nz
.no	Norway	Norid	Not-for-profit corporation	Formal	Legislation[34]	No	http://www.norid.no
.pl	Poland	NASK	Not-for-profit corporation	Formal	Endorsement	No	http://www.nask.pl
.pt	Portugal	FCCN	Not-for-profit corporation			No	http://www.dns.pt /
.sk	Slovak Republic	SK-NIC				No	http://www.sk-nic.sk
.es	Spain	ES-NIC	Part of government	Formal	Legislation	No	http://www.nic.es
.se	Sweden	IIS	Not-for-profit corporation	Informal	Legislation	No	http://www.iis.se
.ch	Switzerland	SWITCH	Academia	Formal	Legislation	No	http://www.nic.ch/
.tr	Turkey	METU	Academia			Yes	http://www.nic.tr
.uk	UK	Nominet UK	Not-for-profit membership corporation	Informal	Advisory	No	http://www.nic.uk
.us	US	NeuStar	Operated by the private sector under contract	Formal	Contract	Yes	http://www.nic.us
.ar	Agentina	Nicar	Part of government	Formal	none	No	http://www.nic.ar/
.br	Brazil	Comité Gestor do Internet do Brazil	Multistakeholder	Formal	Participates	Yes	http://www.nic.br/
.cn	China	CNNIC	Part of government	Formal	none	No	http://www.cnnic.cn
in	India	NIXI	Not-for-profit corporation	Formal	none	No	http://www.nixi.org/
.com	Commercial	VeriSign	Private sector	Informal	N/A	Yes	http://www.verisign-grs.com/
.org	Organisation	Public Interest Registry (PIR)	Not-for-profit organisation	Informal	N/A	Yes	http://www.pir.org/
.net	Network	VeriSign	Private sector	Informal	N/A	Yes	http://www.verisign-grs.com/
.biz	Business	Neulevel	Private sector	Informal	N/A	Yes	http://www.neulevel.biz/
.info	Information	Afilias	Private sector	Informal	N/A	Yes	http://www.nic.info/gateway/
.name	Name	Global Name Registry (GNR)	Private sector	Informal	N/A	Yes	http://www.nic.name/

1: Entity type as self defined by the registries on their websites.
2: indicates whether a formal agreement between the government and the registry exists.
3: ccNSO membership as of 1 September 2006, http://ccnso.icann.org/applications/summary-approved.shtml and *Source*: Registry websites and ICANN website.[35] http://ccnso.icann.org/applications/summary-new.shtml.

Box 2. The land rush for new .eu regional domain names created over 1. 5 million .eu names

.eu is one of the latest country code TLD name additions.[36] .eu already counted over 1.5 million names after only one week of opening to the public and in September 2006 counted over 2 million.[37] The Brussels-based European Registry of Internet Domain Names (EURid) received 350,000 applications involving the validation of "prior right" claims invoked by domain name applicants during the so called "Sunrise Period" at the launch of .eu on 7 December 2005.[38] EURid received a further 702,684 applications during the first four hours it was open to all (so called "land rush period") on 7 April 2006. The five registries of the ccTLDs for Belgium, Czech Republic, Italy, Slovenia and Sweden form the members of EURid, which is the not-for-profit registry for .eu. [39]

To protect the TLD from cyber-squatting and to help guarantee .eu would be well run, applicants during the sunrise period had to not only apply via one of the more than 1 000 accredited registrars, but also send in documentary evidence proving their prior right. Applications and evidence were reviewed by intellectual property experts at PricewaterhouseCoopers in all the different member states before decisions were taken, after which accepted domains were quarantined for 40 days, during which time alternative dispute resolutions (ADR) could be filed. Only then were the names activated. [40]

During the.eu top-level domain land rush, EURid and several industry players believe that "special purpose" registrars were in breach of their registrar contract as they syndicated registrar accreditations to systematically acquire a large number of valuable domain names with the obvious intent of selling them. [41] The requirements to be a .eu registrar were *i)* a certificate that they were an individual business entity and were only applying for one registrar accreditation, *ii)* a certificate that they were offering registrations to their customers on an equal basis and; *iii)* a deposit of EUR 10 000. EURid took action: the registry suspended 74 000 .eu domain names and sued 400 registrars for breach of contract.[42]

ccTLD characteristics and structures

Hierarchy of the TLD and sub-domain policies

ccTLDs have a wide range of structures, some having several levels of hierarchy, which may be structured geographically or generically, and others having flat structures. Most registries that provide registrations under both the TLD and under second-level domains (SLDs) differentiate the two offerings with different rules and pricing.

The DNS uses a hierarchical naming system, with a "fully qualified domain name" representing the hierarchy beginning at the right end of the string and working to the left (*i.e.* server-name.Third-Level-Domain-name.Second-Level-Domain-name.Top-Level-Domain-name). Top-level domains are subordinate to the "root" or "dot" which is the starting point for the hierarchy. [43] While it is possible to register names under the top-level domain in most registries today (*e.g.* directly under .ie or .es), some registries also provide alternative third-level domain name registrations under second-level domains, where different policies or prices may be in effect. Second-level domains often reflect gTLD labels, such as .com/co.xy for companies, .org.xy for organisations, .gov/.gouv/.gob.xy for governmental agencies, .edu.xy for universities and .id/.name/.nom/.me.xy for individuals (where xy represents the 2-letter country code).

Domains names sold under second-level domains are called third-level domains and different policies or prices may be in effect across the various second-level domains. For example, Australian users must choose the category appropriate to their status: com.au for commercial organisations, asn.au for associations, id.au for individuals, and so on. Other second-level domains include .game.tw (for Taiwanese games sites), .asso.fr (for associations in France), .mil.ar for Argentinean military and so forth.

Some registries, in particular in large countries, also create geographic second-level domains. Hence domain names under .la.ca.us are for the city of Los Angeles of the State of California of the United States and domain names under .bj.cn are for Beijing, China.

ccTLDs that function as gTLDs and vice-versa

The apparently simple distinction between gTLDs and 2-letter ccTLDs can often be complex. The differences among TLDs include not only whether a TLD was originally associated with a country code or a generic category, but also with the differences in the policies under which they operate.

Some ccTLDs, usually small countries or islands, actively seek global registrants to generate revenue and function commercially like gTLDs. They do not have technical autonomy on the global Internet but may have relative autonomy as, although they are subject to national regulations of the country or the region in which they are based, they are not subject to the rules that the ICANN community develops for commercial gTLDs. Often referred to as "open ccTLDs" or "quasi-generics", TLD registries that decided to open their name spaces to all interested registrants, regardless of country, include by way of example, .cc (Cocos Islands), .tv (Tuvalu), or .ws (Samoa). The domains .tv and .cc are delegated to a company that is a subsidiary of VeriSign and that markets them globally.[44] It is true, of course, that some ccTLDs lend themselves to marketing toward a certain community with .tv for the television community being a prime example.[45] For the countries or communities concerned there may be significant rewards. The lease of .tv can provide Tuvalu, a Pacific Island nation with a population of 11 000, with significant revenue in the form of royalties, with .tv domain names priced at USD 35 per year.[46] Samoa, another Pacific island nation with a population of 178 000 and 3 000 Internet users in 2002, markets .ws directly to the "web site" community and handles registrations locally.

Niue is a small island in the South Pacific with a population of about 1 200. Its ccTLD, .nu, is popular in Sweden where "nu" means "now" in Swedish. An American entrepreneur acquired the rights to operate and sell the .nu domain name in the late 1990s.[47] He has reinvested some of revenue from the sale of domains to provide Niue with free Internet access. Some current government officials, however, would like a greater share of the registry's income and greater control over the domain name. This prompted a three-year independent investigation the conclusion of which temporarily ruled in favour of the entrepreneur.[48]

Moldova's .md service and the online medical community

The combination of letters in Moldova's code, .md was expected to appeal to doctors in the United States. The Moldovan administrator granted an American company the rights to licence .md domains, hoping to raise revenue for Moldova's struggling economy. MaxMD licensed the right to market .md in more than 90 countries (though not in Moldova itself). The company's goal is to create a full-fledged online community of healthcare providers.

.md currently has registered over 11 000 addresses, including individual physicians and practices, hospitals (including the Mayo Clinics at www.mayo.md), medical organisations (including the National Institutes of Health, which owns www.physician.md), and companies, including Merck or Eli Lilly as well as Moldavian sites. "If the new medical domain really takes off, it could offer a new range of opportunities for communicating with physicians and patients. The experiment seems promising enough that pharma-marketers need to be aware of it—and perhaps start thinking about addresses they anticipate needing in the future".

Source: *Pharmaceutical Executive*, Mar2006, Vol. 26 Issue 3, p152-154.

While some ccTLDs function as gTLDs, some gTLDs function like ccTLDs: .edu, .gov, .mil. All three are limited to registrants from specific communities in the United States – higher educational institutions[49], civilian government agencies, and federal military agencies.

Commercial policy: direct registration or registry-registrar system

A significant policy difference between some ccTLDs and gTLDs is that an indefinite contractual relationship can exist between the domain holder and the registry. All gTLDs have a fixed contract term. Examples of registries that do not include time limits in their contracts with registrants include the Austrian (.at) TLD registry, nic.at or the Netherlands' (.nl) registry, SIDN.

Another significant difference between some ccTLD and gTLD registries is that some ccTLD registries are the actual checking interface/database for registration of new names, even when the new names registration requests are handled via registrars. This means that an interface provides registrars with automatic access to the registration system of some ccTLDs such as .de, so that they can register domains under these TLDs directly.[50]

Many registries, especially in developing countries, do not have registrars. Many other registries offer a registry-registrar system, which introduces a wholesale and retail market for domain names; allowing the registry to focus on providing service to a small group of experienced providers, who in turn provide end-user service to domain name holders. The larger registries have many registrars and extensive resale networks. As documented in OECD (2003)[51], out of the registries that accept direct registrations from the public, some also accept applications through registrars that they have accredited, in which case different levels of pricing are generally applied. Others accept registrations only through registrars, which they have accredited.

Experience shows that a fairly small number of registrars have often better understood the process and captured the market for premium domains upon creation of new top-level domains, upon relaxation of pre-existing regulations in TLDs, or upon deletion of names from registries. Large ccTLD registries that have significant numbers of accredited registrars are also seeing the types of behaviour that have characterised large gTLD registries and which some qualify as “gaming the system”. In some cases, when registrars have direct access to the registry databases, they query ccTLD databases in order to secure valuable names when a new ccTLD or new SLDs are introduced, or to determine which domain names are close to expiration and will soon be deleted from the registry, in cases where the contractual relationship between the domain holder and registry has a finite length. As a result Internet users, including consumers and business, may be unaware that some registrars have “better odds” because they aggregate accreditations. In addition, where domain name speculators are advantaged by such a gaming of the system, the cost to consumers and business of securing the name they want on the secondary market is increased.[52]

In many countries, country code registrars may have to be accredited. Over 250 registries hold the definitive databases of domain names. This can make it very difficult for companies that operate globally if they need to register each name in each ccTLD individually. There are different levels of registrar accreditation. Some registries ask a prospective registrar to pay a fee and sign a contract, in order to become an accredited registrar, while others request a specific code of conduct. The domain .it for example has some 3 000 accredited registrars.[53] Furthermore, several Internet Service Providers, such as VeriSign, have established agreements with many ccTLDs to provide their customers with worldwide brand protection schemes.

Outsourcing registry services

Many of the smaller ccTLD registries outsource the technical management of their registry. A number of companies provide registry solutions for top-level domain managers. Some are complete and integrated, and include data center and systems support as well as managed DNS services and managed names. Ireland-based Afilias is a strong player in providing registry services for both gTLDs (.info and .org) and ccTLDs that include .ag (Antigua and Barbuda), .gi (Gibraltar), .hn (Honduras), .in (India), .la (Laos), .sc (the Seychelles), and .vc (St. Vincent and the Grenadines). Afilias also provides ancillary support to other domains, including .sg (Singapore) and .bz (Belize). Other providers of registry services include VeriSign and Register.com (through Registry Advantage).

ccTLD delegation and administration

While most gTLDs are operated under rules set by ICANN and the agreements by ICANN with registries and registrars, the ccTLDs are separately operated under the rules of each ccTLD. The rules and policies used to administer ccTLD domain names vary significantly and are further documented in OECD (1997) and OECD (2003).[54] A number of important policy choices of ccTLDs in OECD and other countries include:

1. Whether a local presence is required to qualify for the right to register a domain name.
2. Whether there is a limit to the number of domain names for which any single entity can apply.
3. Whether there is an explicit policy in regard to trademark issues and dispute resolution.
4. Whether a Whois database is publicly available.

While many top-level domains started with a strictly regulated policy, few of the ccTLD domain name policies remain that way – reflecting the general move towards more liberalised domain name policies that has taken place over time and in particular compared to the 1997 benchmark when the OECD first documented registry policies. According to a CENTR survey (2005)[55], most CENTR-member registries (65.7%) do not have any restrictions on who is allowed to hold a domain name and most CENTR-member top-level domain registries do not set limits on the number of names an applicant – individual or legal entity – may hold. Most register domains on a “first come, first served” basis. Many registries differentiate requirements for different types of entities registering domain names under different categories of second level domains.

Presence requirements

For registries that require a local presence, the most popular requirement is that there be a legal entity (*i.e.* organisation or corporation) registered under relevant laws of the country. Many countries will accept a registration if the administrative/technical contact is local, although the owner might be elsewhere. For individuals, there are two types of requirements: nationality requirements and local address requirements. Nationality requirements mean that applicants, when acting in a private capacity, must have the nationality of the country where they want to register a ccTLD domain name. Local address requirements mean that applicants must have legal and existing residency in the country.

Rights to a name and quantity of domain names

While a majority of the top-level domains allows an unlimited number of domains per applicant, the degree of requirements for the applicant varies. A few registries require the applicant to document rights to the domain name (Australia is an example in the case of .com.au). A large majority of registries do not require any documentation of rights by registrants. Some of these registries may, however, require either a local presence, or that the applicant be an organisation (or both).

Organisations can generally register an unlimited number of domain names in most countries. In Japan, second-level domains such as ".co.jp" or ".or.jp" are limited to one per organisation. Under the general-use domain name ".jp", users can register an unlimited number of second-level names. In Iceland, there is a difference between domestic applicants and foreign applicants, whereby domestic applicants can register an unlimited number of domain names but foreign applicants are limited to one name per trademark held.

Table 2. Restrictions in ccTLD registration through OECD countries

cc	Location Requirements		Restrictions on Number of Domain Applications	
.au	Yes	Domain name licences may be allocated to an applicant who is Australian, registered or incorporated in Australia as defined under the eligibility and allocation rules for each SLD. Overseas entities with an appropriate trademark or business presence in Australia can also register.	No	Seven second-level domains (SLDs): asn.au, com.au, edu.au, gov.au, id.au, net.au and org.au.
.at	No	No local presence required. Nic.at does not allow PO Box address for contacts.	No	No naming restrictions.
.be	No	No local presence required.	No	No naming restrictions. Available to individuals, businesses, organisations and institutions.
.ca	Yes	Registrants must fall into one of the following categories to qualify as having a "Canadian Presence": (a) Canadian citizen; (b) Permanent resident, (c) Legal representative of (a) or (b); (d) Corporation; (e) Trust - with respect to (a) to (d) above; (f) Partnership; (g) Association; (h) Trade union; (i) Political party; (j) Educational institution; (k) Library, Archive or Museum; (l) Hospital; (m) Her Majesty the Queen. Her Majesty Queen Elizabeth II and her successors; (n) Indian band; (o) Aboriginal Peoples; (p) Government; (q) Trade-mark registered in Canada; or (r) Official marks.[56]	No	
.cz	No	No local presence required.	No	
.dk	No	No local presence required.	No	
.eu	Yes	Location requirements outlined in Article 4.2.b of Regulation 733/2002[57]: *(i)* undertaking having its registered office, central administration or principal place of business within the (European) Community, or *(ii)* organisation established within the (European) Community without prejudice to the application of national law, or *(iii)* natural person resident within the (European) Community.	No	
.fi	Yes	Registrants must be judicial persons properly registered in Finland or private persons who have a Finnish Personal Identity Number and are domiciled in Finland.	No	Some naming restrictions exist.
.fr	Yes	A domain name within the ".fr" naming zone can be attributed to any requesting body officially registered in France or to individual swith an address in France.	No	
.de	Yes	If the domain holder does not have his residence in Germany, the admin-c at the same time is the person authorised by him to accept service under the aspect of §§ 174 f. ZPO (Code of Civil Procedure); in this case he in turn must have his residence in Germany and has to state his serving address.	No	Available to individuals, businesses, organisations and institutions.
.gr	No	No local presence required.	No	
.hu	No (depends on SLDs)	1) Registrants of the .hu public domain can be any Hungarian citizen or any natural person with permission to reside in Hungary, or any organisation or enterprise with a geographical address in Hungary or an owner of a trade mark registered by the Hungarian Patent Office - even in the case where he/she is not a Hungarian citizen. 2) Registrants of a second-level public domain can be any Hungarian or foreign natural or legal person or an organisation with no legal personality.	No	
.is	Yes	All domestic legal entities properly registered in Iceland are eligible to apply for a domain. Foreign applicants, who are not domiciled in Iceland, can apply for a .is domain on the basis of: *i)* Owning a registered trade mark at the Icelandic Patent Office. Only one domain may be applied for on the basis of each trade mark. The trade mark must consist of letters or numerals exclusively. The applicant must specify an Icelandic agent administrative contact for the domain. *ii*) Holding an international legal status or being internationally regarded as having such status. Examples are foreign embassies, organisations constituted under international law and international sports federations. The applicant must specify an Icelandic agent administrative contact for the domain.	No	Foreign applicants can apply for as many names as they want, one based on each trademark they hold.
.ie	Yes	*i)* An applicant who is a natural person, and can show documentary evidence or reasonable proof of a correspondence address within the 32 counties of Ireland (the island of Ireland) along with adequate documentary evidence of the applicant's legal name *e.g*: a copy of the applicants' passport or birth certificate, shall be deemed to have a real and substantive connection with Ireland. *ii*) An applicant which, at the time of application, is a body corporate incorporated under the laws of Ireland shall be deemed to have a real and substantive connection with Ireland or *iii*) An applicant which, at the time of application, is a body corporate incorporated outside Ireland and which has either established a "place of business" within Ireland which it has registered under Part XI of the Companies Act 1963, or has established a "branch" in Ireland which it has registered pursuant to the European Communities (Branch Disclosures) Regulations, 1993 shall be deemed to have a real and substantive connection with Ireland.	No	

cc	Location Requirements		Restrictions on Number of Domain Applications	
.it	Yes	Domain names within the ccTLD ".it" can be assigned to subjects belonging to a member state of the European Union.	No	No limit for individuals. Companies can register multiple domain names but must supply a VAT number.
.jp	Yes	The Registrant must have a Japanese local presence with a home or office address.	No (depends on SLDs)	Unlimited for .jp. Limited to one per organisation for second-level domains such as ".co.jp" or ".or.jp".
.kr	Yes	Registrants must have an office or domiciles in Korea. If the applicant is a company, a Certificate for Business Registration is needed in order to register a domain name.	Yes	One domain name per private person.
.lu	Yes	The administrative contact has to be established in Luxembourg. Domain name holders which are established outside Luxembourg are therefore obliged to give valid power to an agent who is established in Luxembourg for the registration and the management of their domain name.	No	
.mx	No	No local presence required.	No (depends on SLDs)	No naming restrictions for .com.mx. Restrictions for other SLDs.
.nl	No	No local presence required.	No	No limit for companies or for persons. List of reserved names.
.nz	No	No local presence required. Available to individuals and businesses. Registrant must be an identifiable individual over 18 years of age or a properly constituted organisation. .co.nz for commercial organisations; .net.nz for NZ Internet Organisations and service providers; .org.nz for Not-for-profit organisations.	No	
.no	Yes	The applicant must be an organisation registered in the Enhetsregisteret (the Central Coordinating Register for Legal Entities). The organisation must have a Norwegian post address. Individuals may register domain names only under "priv.no".	No (depends on SLDs)	Up to 20 .no domain names per organisation directly. Up to 5 domain names under each geographic domain. Up to 5 domain names under each generic domain to which it belongs.
.pl	No	No local presence required.	No	No naming restrictions under .pl, .com.pl, .net.pl, .org.pl, .biz.pl and .info.pl
.pt	No	No local presence required.	No	
.sk	Yes	The company needs to have its representation in the Slovak Republic. Domain can be used only in relation to networking in the Slovak Republic.	Yes	Up to 5 domains per company.
.es	No	Domain names under ".es" (and under ".com.es", ".nom.es" and "org.es") can be allocated to any natural or moral person that has an interest in Spain, or maintain links with Spain. More specific location requirements only apply to "gob.es" and ".edu.es".	No	SixSLDs:.es,.com.es, .nom.es, .org.es, .gob.es, .edu.es
.se	No	No local presence required.	No	
.ch	No	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 top-level domains only for entities located in Switzerland.	No	
.tr	No	No local presence required.	No	
.uk	No	No local presence required.	No (depends on SLDs)	No naming restrictions .org.uk, me.uk, co.uk.
.us	Yes	One of the following eligibility requirements must be met: 1) A natural person (i) who is a citizen or permanent resident of the United States or any of its possessions or territories or (ii) whose primary place of domicile is in the United States of America or any of its possessions, or 2) Any entity or organisation that is incorporated within one of the fifty (50) U.S. states, the District of Columbia, or any of the United States possessions or territories or (ii) organised or otherwise constituted under the laws of a state of the United States, the District of Columbia, or any of its possessions or territories, or 3) An entity or organisation (including federal, state, or local government of the United States, or a political subdivision thereof) that has a bona fide presence in the United States.	No	

Trademark policies

It is important to note that cybersquatting cases have evolved considerably since the colossal explosion of domain names registration at the end of the 90s. The registries in all OECD member countries provide some trademark policies. The majority of registries explicitly stipulate that registrants must take all responsibilities related to trademarks and other rights of third parties in domain name registrations. This is because the most common rules for domain registrations are "first come, first served" basis and most registries or registrars do not check whether applications violate trademarks or other rights of a third party. In cases of conflict between a registrant and a third party, registries try not to get involved in conflict resolution. However, it is standard for registries to provide dispute resolution policies for domain names, particularly for the most common or predictable types of litigations, and reserve the right to take necessary action. An example of such action might be to cancel a registration, according to results from regulated resolution processes. National and regional intellectual property offices have created a number of on-line trademark databases and have made them accessible to the public through their websites. The World Intellectual Property Organization (WIPO) provides access to many of these databases with a view to the prevention of domain name disputes.[58]

Dispute resolution

Regardless of the evaluation performed by the registry and as previously stated, final responsibility for domain name choice resides with the applicant. For most registries, the regular conflict procedure is to inform the parties how to get in touch with one another, but to otherwise refrain from any involvement in a conflict. It is worth mentioning the "wait status" for .at domains as an example, which prevents changes in domain holders for a certain period of time, during which negotiations between the domain holder and the complainant can take place.

Many top-level domains have some form of alternative dispute resolution in place. Some ccTLDs, such as the ccTLD registry for the United Arab Emirates (.ue) or French registry (.fr) have implemented the WIPO Uniform Dispute Resolution Process (UDRP), whereby WIPO's Arbitration and Mediation Center Mention administers dispute procedures for a ccTLD registry.[59]

Most of the large ccTLDs have enhanced alternative dispute resolution procedures or services that are different from WIPO's UDRP and are tailored to local needs.[60] Examples include Nominet's (.uk) Dispute Resolution Service or CIRA's (.ca) dispute resolution process.[61] In addition, in a number of cases, separate procedures for individuals have also been implemented.

Even when alternative dispute resolution mechanisms are in place, the use of local courts is possible in parallel to the alternative dispute resolution (ADR) procedure offered. In the absence of ADR mechanisms, conflicts are addressed by means of the legal system in accordance with the applicable legislation on name rights. A drawback is that this may be a time-consuming process, and in some cases, it has been difficult to determine which jurisdiction applies.

CURRENT AND ONGOING CCTLD POLICY AND TECHNICAL ISSUES

Internationalised domain names: opportunities and challenges

Internationalised domain names (IDNs), *i.e.* supporting non-ASCII characters in domain names, can help to make it possible to use one's own language scripts to type in domain addresses[62] and help businesses or other entities gain local recognition by having domain names in local language. Therefore, IDNs are a part of the efforts pursued to promote multilingualism on the Internet. An opportunity for most stakeholders such as users, companies, or registrars, IDNs also represent a challenge, depending on how IDNs are implemented and which accompanying policies are developed. For instance, companies with trademarks may need to engage in additional defensive registrations if policies are not in place to solve these issues, and some areas in the application layer of the DNS might not work well with IDN top-level domains. While there are claims that existing technologies for IDN work well and that barriers to implementation are low, many consider that introducing IDN, in particular IDN in top-level domains, is a complex process that requires significant co-operative efforts and testing if it is to be done while preserving the stability of the domain name system and of the Internet.[63]

The demand for IDN is based on the desire to increase access to the Internet to most of the world's population, which does not use or recognise ASCII characters and on the related wish for Internet identifiers to reflect cultural variety. Some countries are actively involved in promoting IDNs, as strategic to local populations' uptake of the Internet. The estimated proportion of English speakers is below one-third of the Internet population. Chinese language speakers represent the second largest group of Internet users at 13%. Japanese represent 8.5% and Koreans 3.3%. Russian, Chinese, Indian, Arabic, Greek, Hebrew, Thai, Japanese, and other Internet users do not use the Roman alphabet.[64] Indicative of the importance of multilingualism to many countries, the Saudi input to the Internet Governance Forum (IGF) that was created as an outcome of the World Summit on the Information Society (WSIS), states "Multilingualism is critical to increasing access to and use of the Internet".[65]

As mentioned in the Saudi submission for IGF planning, multilingual domain names, e-mail addresses, keyword lookup, as well as multilingual content, are four distinct areas in which improvements would make it easier for all language populations to benefit from the Internet. Efforts to support multilingual access to the Internet and to co-ordinate work across different countries, regions, and language groups are welcome and ongoing. Of particular interest in many countries is access to the Internet and the DNS using home-country languages. Domain names were originally limited to ASCII characters, using the "A-Z" characters from the Latin alphabet, and 0-1 and the "-". The Unicode system has been standardised internationally and handles nearly a million characters expressing almost every character in most widely-used languages, including Latin, German umlauts, Hebrew, Arabic, Greek, Cyrillic, Korean, Thai, Hindi and pictographic languages such as Chinese and Japanese. The Unicode system is often upgraded to document the scripts that characters belong to.

The IDNA solution

While some experts originally argued for a major overhaul of the Internet's infrastructure to incorporate IDNs, pressure to act quickly reduced support for solutions that would require extensive changes in architectures or standards: the result was an effort led by the IETF (Internet Engineering Task Force) that resulted in the Internationalising Domain Names in Applications (IDNA) mechanism.[66] IDNA enables end-user viewing of IDNs without altering the existing domain name system: Unicode strings are incorporated into domain names. [67] A scheme called punycode encodes Unicode characters as ASCII strings, before placing the ACE prefix "xn--".[68] Thus Unicode strings are mapped into ASCII code strings of the form "xn--<ASCII sequence>", for example, 万维网.娱乐.cn (which means entertainment.cn in Chinese), becomes xn--chqs60j8ha.cn.[69] Hence, IDNs are simply domain names written as "xn--xyz.cc". IDN resolution is based on the distribution of client software and does not modify the server side operation.

There are many groups working on IDNs, including but not limited to i-DNS.net, MINC (Multilingual Internet Names Consortium, formed in June 2000), UNESCO (United Nations Educational, Scientific and Cultural Organization), ACALAN (*Académie Africaine des Langues*), IETF (Internet Engineering Task Force), IAB (Internet Architecture Board), JET (Joint Engineering Team) or ITU (International Telecommunication Union). ICANN's GAC (Governmental Advisory Committee), gNSO (generic Name Supporting Organisation) and ccNSO (country code Name Supporting Organisation) are also actively working on IDNs. Language groups, which develop their own language and variant tables, and co-ordinate with each other on these tables include JDNA (Japanese), CDNC (Chinese), INFITT (Tamil), EuroLINC (European Languages), CYINC (Cyrillic), GLWG (Georgian) and working groups for other languages including Arabic and Urdu.

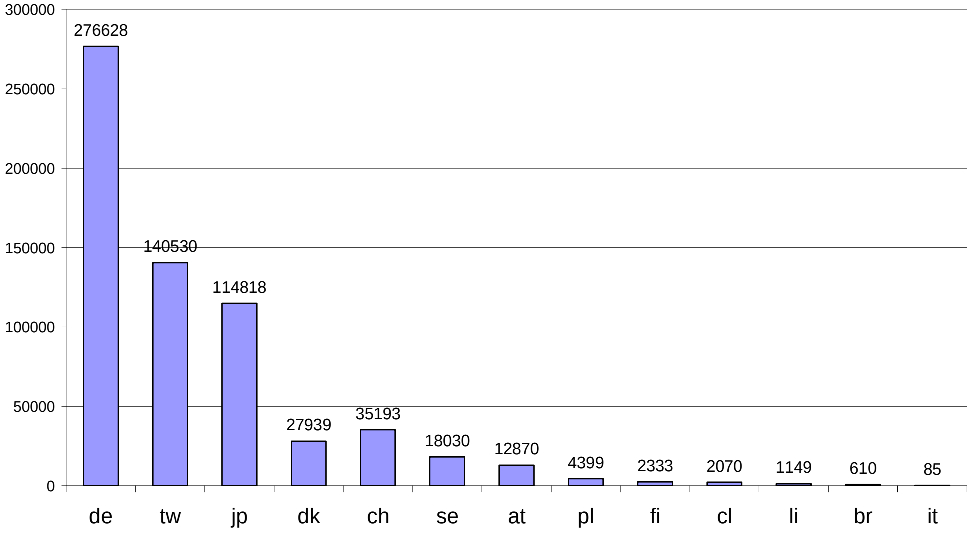
Registry implementation of IDNs and initial demand for IDN

CcTLD registries have been implementing IDN since 2000.[70] Compared to ccTLD registries, gTLD registries have higher restrictions on IDN implementations, as they need to follow the IDN Guidelines[71]. Large gTLDs including Afilias or VeriSign are actively involved in the IDN debates and standards. The current issue is that of putting in place processes for development, maintenance, upgrade and IDN resolution in applications that use uniform syntax/semantics throughout all applications.

The current IDN standard for domain names containing letters with diacritics or characters from non-Latin scripts such as Arabic or Chinese has been implemented by several registries so far, including ccTLD registries in China, Japan, Korea, Chinese Taipei, Poland, Switzerland, Germany, or Austria, and by the gTLDs registries for .net, .org, and .info. The Brazilian Registry (.br) now allows registration of Internationalised Domain Names (IDNs) containing Portuguese special characters, mainly the punctuated symbol cedilha" "ç" and the accented vowels: acute (example: "á"), circumflex (example: "â"), grave (example: "à"), and tilde (example: "ã"). The Greek registry also permits the registration of Domain Names in Greek characters. The Indian government is working on a roadmap to implement multi-lingual domain names under the Devnagari and Dravidian Indian scripts. Beyond implementing IDNs, registries are actively planning DNS resolution, domain registration, and interim resolution strategies for Whois.

In Chinese Taipei, IDNs account for nearly 50% of registrations.[72] On the other hand, Germany implemented IDNs but there was not much demand. In the German-speaking countries, IDNs now have a market share of 3-4%. Similarly the local Internet communities of countries like France, Italy or the Netherlands do not view IDNs as a priority. According to CENTR (2005), 48.6% of its member registries allow IDN registrations today. [73] Of these, 55.6% are registered in their IDN form (44.4% are registered in the "xn—form"). According to another survey by CENTR, 21.5% of CENTR-member registries that have implemented or plan to implement IDN also plan a sunrise period for trademark owners and 50% plan a landrush. A project by King Abdul Aziz University in Saudi Arabia is implementing Arabic domain names with other universities in the Gulf region with plans to expand it to other Arab countries.[74]

Figure 8. IDN registrations on 31 October, 2005



Source: Denic.de – Domain Pulse, 2006, Berlin, and JPRS registry statistics for 31/10/2005.

IDN client issues

Until now, the use of IDNs was hindered by the fact that the market leader amongst Internet browsers, Microsoft’s Internet Explorer, has not been able to display them. Microsoft’s new Internet Explorer 7.1 now supports IDNs, overcoming this barrier for its users. But web browsing is not the only factor to consider when planning for IDNs. Other software applications and e-mail systems need to be compatible whilst most applications currently include a check that ensures a domain name excludes all but ASCII. Client manufacturers of browsers, mail clients, and mail servers raise technical and adoption issues. The issues involved with supporting keywords are the same as domain names. But e-mail clients cause a specific problem, in particular the portion of the name that is on the left of the “@”. Supporting the left hand-side of multilingual e-mail addresses is more complex than the right-hand side, because a range of characters including spaces, upper cases etc. can be accepted. Ideally, one could have IDN@IDN.IDN, but technically that is some years off in development. Even if the latest name server and latest browsers supporting IDNs were available widespread roll-out would still take many years.[75] That being said application developers should take these developments into account and plan actively for IDN resolution.

The IDNA mechanism solves only part of the multilingualisation problem. Remaining to be addressed are the questions of potential consumer confusion; conflict avoidance or resolution for similar-appearing names; internationalisation of e-mail addresses; differences in interpretations for different languages; restrictions on registrations on a per-domain basis; implications for the UDRP and the Whois database (of information about domain name registrants); security issues raised by IDNs; the implications of (and alternatives to) multilingual top-level domains; and the actual availability of content in the numerous languages, alphabets, scripts and character-sets that need to be addressed.

Implementing IDN at the top level

While IDN is still limited to the second-level domain (*e.g.* IDN.jp) rather than also at the top-level domain (IDN.IDN), a program is in place at ICANN to test IDN TLDs.[76]

At the technical level, two methods for supporting internationalised TLD labels have been proposed:

1. One solution; that of "IDN TLDs", applies the IETF IDNA (Internationalising Domain Names in Applications) standards in the composition of top-level domain names. IDNA accommodates the use of Unicode-encoded characters in the composition of domains. It defines a method for encoding labels containing non-ASCII characters using only the "letter-digit-hyphen" subset of ASCII characters already allowed in the DNS for backward-compatibility so that "internationalised" domain names can be introduced with minimal changes to the existing infrastructure.

2. A second solution[77] also recommends that local or national language equivalents of TLD labels be constructed as ASCII Compatible Encodings as specified in RFC 3492 on Punycode, but that the DNAME construct defined in IETF RFC 2672, Non-Terminal DNS Name Redirection be used to map such name spaces directly onto existing generic and country-code TLDs.[78]

Security issues

Different characters in different languages can look the same, depending on the font used. For example, Unicode character U+0430, Cyrillic small letter a ("a"), can look identical to Unicode character U+0061, Latin small letter a, ("a") which is the lowercase "a" used in English. Characters that look alike in this way may be termed homonyms, homographs, or homoglyphs. The expanded character repertoire increases the scope for "homograph spoofing" attacks, meaning characters that look like something else to trick the user to believe that he/she is at a desired address (*e.g.* www.bank.com) while being on a malicious website (*e.g.* www.bank.com, where "a" is written in Cyrillic while the other letters are ASCII).

This problem was anticipated before IDN was introduced, and guidelines were issued to registries to try and avoid or reduce the problem – for example, recommending that registries only accept the Latin alphabet and that of their own country, not all of Unicode. When the registries allowed only specific code points, there were no problems (an abstract character repertoire is a set of characters, called code points, from one or more alphabets or from one or more scripts which are the set of letters used to write a particular language). IDN "phishing" schemes often happen when registries ignore the guidelines and allow the registration of names in Unicode that contain characters from different scripts similar to characters from another script.[79] Phishing is a form of criminal activity, characterised by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by pretending to be a trustworthy person or business. The term arises from the use of increasingly sophisticated lures to "fish" for users' financial information and passwords.

The Mozilla Foundation has announced changes to Firefox concerning Internationalised Domain Names (IDN) to deal with homograph spoofing attacks. According to the organisation, "Mozilla Foundation products now only display IDNs in a whitelist of TLDs, which have policies stating what characters are permitted, and procedures for making sure that no homographic domains are registered to two different entities.[80] Within the technical community, doubts remain as to whether this approach might deliver a real solution, since even within the scope of permitted characters, phishing will be possible.

ICANN policies for IDN

ICANN, supported by the .cn, .info, .jp, .org, and .tw registries, developed a first series of IDN guidelines for the introduction of IDN on the second-level of the DNS which were published in June 2003, coinciding with the launch of deployment of IDNs under the IETF's Proposed IDNA Standard reflected in RFCs 3490, 3491, and 3492.[81] ICANN provided a second version of guidelines for implementation of the IDN standard for internationalised domain names in February 2006.[82] ICANN is working on the technical test of IDN.IDN with the aim of allowing the registration of IDN.IDN in the future. A joint ccNSO/gNSO working group prepared a paper in May 2006 discussing the issues associated with IDN. Issues and challenges lie in the management and support of specific IDNs, as well as in managing policies for implementing IDNs in the top-level domains.

ICANN has taken IDNs fully toward the end of 2005. ICANN’s Security and Stability Advisory Committee (SSAC) recommended analysis of two candidate methods for encoding strings in TLD labels – DNAME Equivalence Mappings and use of IDNA encodings. The SSAC also recommended the active participation of ccYLD registries in ICANN's, and the active participate in the ICANN IDN Experimental Testbed projects and that ccTLD registries provide their perspectives on the implementation of “internationalised” TLD labels in the root. SSAC recommends that ccTLD registries and national or regional linguistic organisations not implement standalone or alternate TLD schemes until the results of the IDN Experimental Testbed are available.

ICANN released a timetable leading to the technical testing of IDNs at the top-level domain level starting in July 2006.[83] The technical test will include two approaches to the insertion of IDN records into the root zone of the DNS. These are: *i)* DNAME records - as defined in RFC 2672. DNAME provides an alias designation for an entire domain by mapping a new domain into another that already exists. For an existing TLD, this corresponds to the use of a punycode string to provide an internationalised alias designation for that TLD using a DNAME record in the root zone and *ii)* NS-records which permit the insertion of an internationalised label in the top-level domain of the root zone without the duplication of a pre-existing sub domain structure.

The test procedure will ensure that enabling multiple scripts at the top-level will not adversely affect users. It will also establish the technical methods that are available for such deployment and will enable ICANN's policy development bodies to move forward with their ongoing work on accessing the Internet using non-ASCII scripts.

According to ICANN, policy decisions on IDN at the top-level need to be based on the results of transparent and verifiable tests in a test environment of suitable technical bases for the deployment of IDN TLDs. The available solutions need to be both technically stable and not compromise the stability and security of the DNS. Therefore, the result of the technical test is considered to be absolutely essential input to policy development processes. ICANN's Generic Names Supporting Organization (GNSO) initiated a policy development process during the ICANN meeting in Vancouver in December 2005 and issued a prliminary issues report in May 2006.[84] Further work includes participation from the ccNSO and the Governmental Advisory Committee (GAC).

China’s approach to implementing IDN.IDNs

CNNIC has implemented Chinese character versions of top-level domains for .cn 中国, .com 公司, and for .net 网络 since 2002.[85] Administered by CNNIC rather than by ICANN, it operates as would an Extranet. Usage requires downloading a special plugin.

There are two different kinds of Chinese domain names. One kind is IDN.cn and the other kind is three combinations of IDN.IDN: IDN.公司 (.com's Chinese equivalent), IDN.网络 (.net's Chinese equivalent), and IDN.中国 (China's .cn equivalent). For IDN.cn, the IANA root is used to point to .cn. For IDN.IDN, a browser plug-in automatically appends a .cn to the right of IDN.IDN, turning them into IDN.IDN.cn, and still using the IANA root to point to .cn, which is why IDN.IDNs in China are not technically top-level domain names.

Once the plug-in has added a .cn to the domain name, CNNIC’s central resolver fixes all the resolvers locally. (.com .net .cn in Chinese). If a user sends a message out of China, it appends a .CN. The main problem is that mail servers outside China do not know how to respond to these unless users configure their clients.

Chinese is one of the world’s largest linguistic communities and the Chinese seem to associate a strong cultural dimension with IDN.[86] Some 80 million Chinese language plug-ins have been distributed worldwide, of which 80% via direct access by Internet Service Providers (ISPs) that support Chinese-character domain names in China, Hong Kong (China), Singapore, Malaysia, Chinese Taipei, and the United States.

CNNIC claims to be actively participating in the activities for the ICANN planned IDN experiment with its hope to finally register Chinese IDN.IDN in the IANA root and eliminate the plug-in for this purpose.

Whois policies

Whois is a TCP-based query/response protocol, which is widely used for querying a database in order to determine the owner of a domain name, an IP address, or an autonomous system number on the Internet. The most common use of Whois is for finding information about domain name registrations (including name server information, data on registrant, creation date, expiry date, etc.). Publicly available Whois services and Whois data involve a wide and complex range of public policy issues, including consumer protection, law enforcement, privacy, intellectual property protection, as well as technical and registry/registrar management. To date, the use of public Whois data has been both beneficial (for example to verify the availability of domain names for purchase or the identity of an e-commerce merchant) and nefarious (for example to collect e-mail addresses to send spam).

Whois information availability and privacy regulations

All ccTLD registries in OECD member countries, and most but not all other registries provide public access to some form of Whois data, although not necessarily the same data as that required by ICANN from the gTLD registries and ICANN-accredited registrars. Each registry manages its own Whois: for example Afnic manages the .fr Whois. According to CENTR (2005)[87], 89%[88] of all CENTR-member ccTLD registries provide a Whois service. Whois-type databases must necessarily be in conformity with national law on data protection and privacy, which vary across countries. There is not a common interface since each national law dictates which information is “personal data”.

Some registries make distinctions between individual registrants and those registering domain names for commercial purposes. For example, .fr names will be made available to individuals for registration of domain names as of June 2006 and the French data protection authority enables the ccTLD registry to make public on Whois only information to get in contact with the administrative contact person and no other contact information. Nominet, the .uk registry, provides an opt-out to non-trading entities so that entities such as children's groups and individuals can protect their personal data.

One basic reason for which ccTLD registries started providing Whois service on their websites was as the first step for applicants to determine the status and availability of domain names for purchase. Many ccTLD registries, including AusRegistry Ltd. in Australia and Nominet in the United Kingdom, have now set-up separate services to check domain name availability or to check Whois information on a registered domain. Various Whois task forces have also produced recommendations to limit data-mining and restrict the uses of bulk access to Whois data. Some registrars offer registrants anonymous registration using a proxy service, sometimes charging a fee for this service.

The accuracy of the Whois data

The Whois data policies and practices of ccTLDs are intended to provide accurate information regarding domain name registrations consistent with national laws.[89] Whois data is considered as an important information source to help resolve technical issues, and can also be used to protect security, combat illegal activities and identify merchants. The two types of Whois are DNS Whois and IP address Whois. CcTLD registries have no control over IP address Whois, but the DNS Whois could point to an IP address which could then be used for law enforcement. ISPs and network operators use the information in Whois in dealing with day-to-day network operations and in responding to Denial of Service (DOS) attacks. Law enforcement agencies also use Whois in order to combat cybercrime. Consumers might use Whois to verify the identity of an online merchant. However, usefulness of the Whois database is conditional on the data in this database being accurate and there is strong concern regarding the inaccuracy of Whois data. Inaccuracy of the Whois data can be caused by registrants providing fictitious registration information, which can be difficult and burdensome for registrars to verify and not always effective, or by mis-entry of the data or failures to update the information.

The availability of the Whois data

Related to the accuracy of Whois data is the availability of Whois data. Indeed, some registrants, individuals in particular, may provide inaccurate Whois information because they do not wish their personal information to be available online. Other registrants, such as cyber squatters or cyber criminals, do not input accurate data so as to conceal their identity from legal authorities. Options implemented by ccTLD registries include creating a category of names where registrants can elect to not have their details disclosed through Whois. In France, individual registrants under ‘nom.fr’ can choose to have their details be “red-listed” and publicly unavailable in which case technical information such as the ISP and DNS servers is available but no personal information is shown.[90] Another option, implemented by Nominet, the .uk registry, involves a wider opt-out policy whereby consumers may voluntary opt-out of having their address shown through Whois.[91] Some registries (such as .at) offer the option of not displaying some personal data in the publicly accessible Whois database (e.g. e-mail address, telephone number and fax number in the .at example).

Technical solutions have been implemented by many registries to prevent Whois abuses. For instance, traffic monitoring techniques such as query rate limiters have been implemented in a number of ccTLD registries and registrars, to combat specific Whois abuses such as widespread data mining by spammers. Limiting the query rate impedes the massive access needed for many marketing purposes. Individualised determinations of the need to mask some Whois data under special circumstances have been employed effectively by some relatively large ccTLDs. In Australia, to prevent data mining, street addresses are not published and access to the Whois database is limited to 20 per IP address per hour and a total of 200 in a 24-four hour period. In the United Kingdom, registrants are informed when their data is shared, except in the case when the data is part of a police investigation. Australian law enforcement agencies may gain access to more detailed data from AusRegistry Ltd, the .au registry, and Nominet will provide non-public data in response to specific requests from law enforcement agencies on a case-by-case basis. In addition, work has commenced on a new means of querying the registry database known as CRISP. In addition to improved structured query options, this new means enables the identification of the party querying the database as well as appropriately differentiated access authorisations for data content.

Although the range of policy and regulatory environments across gTLDs and ccTLDs prevent the establishment of a universal Whois data provision and access policy, an on-going policy development process on Whois by ICANN's generic Name Supporting Organization has provided the impetus for renewed focus on Whois by the GAC, which is considering general public policy principles applicable to Whois.

Security and DNSSEC

DNSSEC (short for DNS Security Extensions) adds security to the Domain Name System (DNS) used on Internet Protocol networks. The need for improving DNS security stems from the rationale that DNS answers can be modified (domain names can be hijacked) since the DNS relies on a 16-bit "secret" to match answers to questions and that name server caches can be poisoned with inaccurate data. DNSSEC consists of hierarchies of cryptographic signatures for DNS queries and responses that can provide Internet users with origin authentication of DNS data, data integrity, and authenticated denial of existence. DNSSEC does not protect the confidentiality of the data transmitted nor protect against denial of service (DOS) attacks or distributed DOS attacks. DNSSEC-bis, or the DNSSEC specifications, were published in March 2005 and describe the current DNSSEC protocol in detail RFC 4033, 4034 & 4035. Two extensions to this standard have been proposed to make DNSSEC-bis conform to European Union data privacy requirements.[92] The first, published in RFC 4470, is a preliminary solution and requires that DNSSEC keys be applied online on DNS name servers, which some TLDs see as not feasible in terms of resources required. The second, eliminating the enumeration possibility, is under active development within the IETF, with contributions from large ccTLDs. Production level implementations do not exist for either of these approaches.

The decentralised nature of protocol adoption means that various ccTLD registries will make independent implementation decisions and that the migration to DNSSEC will be incremental with new and legacy systems coexisting. The registries in Sweden and in the Netherlands have been on the forefront of DNSSEC deployment efforts.[93] It is expected that major steps towards DNSSEC implementation will be taken within the next 1-2 years. .se, .nl, .gov have made progress, and RIPE NCC, one of five Regional Internet Registries (RIRs), has begun to deploy DNSSEC in its operations.[94]

CCTLD RELATIONSHIPS WITH OTHER INTERNET BODIES

Background

Since November 2000, the United States Department of Commerce (DoC) has contracted ICANN to perform the Internet Assigned Numbers Authority (IANA) functions[95]. Under the IANA functions contract, ICANN receives requests for changes to the authoritative root zone file and makes recommendations regarding them to the DoC, which has oversight responsibility for the authoritative root zone file.[96] In June 2005 the US government released a Statement of Principles on the Internet's Domain Name and Addressing System which included a recognition that governments have legitimate public policy and sovereignty concerns with respect to the management of their ccTLD and a commitment to work with the international community to address these concerns, bearing in mind the need to ensure stability and security of the Internet's DNS.[97] Previously, ICANN in performing the IANA functions would transfer control of a domain-name suffix only if it were "in the best interests of the Internet community" and if both parties agreed to the change, according to its statements. The Governmental Advisory Committee to ICANN (GAC) has recently identified ccTLDs as a key priority area for early engagement.[98] The role of different parties is further detailed in OECD, 2005, "OECD Input to the United Nations Working Group on Internet Governance (WGIG)".[99]

Regional country-code organisations CENTR, APTLD, LACTLD, AFTLD

Regional country code organisations play a strong role in sharing best practices between ccTLDs, in training and in capacity building. Regional organisations also help to address a region's specific joint concerns and participate as observers in ICANN's country code Name Supporting Organisation's (ccNSO) meetings.

The Council of European National Top-level Domain Registries (CENTR) is very active amongst ccTLD registry associations, through the development of surveys, best practices or consensus positions, as well as collaborative projects on technical, managerial and legal issues affecting ccTLDs. The Asia Pacific Top-Level Domain Association (APTLD), an organisation for ccTLD registries in the Asia Pacific region also works as a forum for information exchange on technological, operational, and training related issues between domain name registries in the Asia Pacific region. For example, in 2006 APTLD is establishing a ccTLD managers' training school in Thailand.[100] APTLD is very involved in Internationalised domain names (IDNs) and has its own working group on IDNs. LACTLD for the Latin America and Caribbean region was created in 1998 in Argentina with the objective of fostering communication between the region's ccTLDs, and the African Top-level Domains Organization (AFTLD) was launched in 2002 in Mauritius.

The relationship between governments, ccTLDs and ICANN

While the regional ccTLD organisations stimulate best practices and can address issues that are specific to a region, ICANN's Country Code Name Supporting Organisation (ccNSO) is a forum to represent the ccTLD community within ICANN and its other constituencies, in particular the Governmental Advisory Committee to ICANN (GAC) and ICANN's gNSO.[101] It is important to note that in comparison to the GNSO, the ccNSO is still at an early phase in its institutional development.

The relationship between ccTLDs and ICANN

Acceptance by ccTLD registries of ICANN's role regarding them is still considered by some to be a critical challenge in establishing an ICANN that is viewed as a legitimate steward for the DNS. Some question whether there are global ccTLD issues, hence whether an international organisation need have a substantial role in the ccTLD area. Others point to the importance of giving a voice and influence to the ccTLD registries in ICANN's policy development processes.

An essential role that ICANN has vis-à-vis the ccTLD registries is DNS root zone file management, as part of the IANA functions. A minority of ccTLDs have formal agreements with ICANN[102], although the larger registries have regular technical arrangements and interactions with ICANN through the IANA functions. The administrative activities comprising DNS root zone file management include receiving requests for and making routine updates of ccTLD contact and nameserver information. These activities also include receiving delegation and re-delegation requests, investigating the circumstances surrounding those requests, and making recommendations and reporting actions undertaken in connection with processing such requests.

The Accountability Framework document is designed to cater to ccTLD managers who require a more 'formal' document with ICANN but do not want to join ccNSO or sign a full-fledged contract. It constitutes a mutual recognition and commitment of both parties, covers dispute resolution and termination, financial contribution to ICANN on a yearly basis, subject to review and contains a termination clause. For ccTLDs who are more comfortable with simple statements of commitment, another option to formalise their relationship with ICANN is an exchange of letters.

The relationship between some ccTLDs and ICANN has not always been to the satisfaction of all parties.[103] Issues associated with sovereignty and ccTLDs have related to a large extent to issues of delegations and re-delegations. The issue of financial contribution of some ccTLDs to ICANN's budget is not yet resolved. The ccNSO has established two working groups: the fee apportionment working group and the budget working group. While the first has concluded its work, the second is working on providing ccTLDs with costs associated to ICANN in performing the IANA functions that are in the interest of ccTLDs (see discussion below on the IANA function: day-to-day technical operations). The process is ongoing.

The creation of the ccNSO

Under its 2003 reorganisation, ICANN replaced the Domain Names Supporting Organization with two organisations: the gNSO and the ccNSO, in which the ccTLDs would be more actively involved.

Being a member of the Country-Code Names Supporting Organization is independent from entering into "Accountability Frameworks" with ICANN or exchanging letters of recognition as it entails developing policies that are binding for ccNSO members within the limits of national law. Out of the 264 ccTLDs, the ccNSO currently has 55 ccTLD members[104], 8 of which are from the ICANN Europe zone, 15 are from the Africa zone, 13 from Latin America and the Caribbean, 15 from the Asia-Pacific zone, and 4 from North America.[105] Organisationally, the ccNSO Council has the authority to appoint the same number of members to the Nominating Committee (NomCom) for ICANN's Board, as the gNSO, and as the at-large constituency (ALAC) (See Annex 1 for a representation of ICANN's organisational structure and the composition of ICANN's NomCom).

The Country-Code Names Supporting Organization (ccNSO) is aimed to be a policy-development body responsible for *i)* developing and recommending to the Board global policies relating to country-code top-level domains; *ii)* Nurturing consensus across the ccNSO's community, including the name-related activities of ccTLDs; and *iii)* Co-ordinating with other ICANN Supporting Organizations, committees, and constituencies under ICANN.[106] The ccNSO policies are binding for their members unless they contradict local law. ccNSO priority discussion issues include the IANA functions, the development of guidelines for ccTLD managers, best practices, finalising the policy development process, a joint working group with GAC, as well as outreach activities.[107] Other areas of policy development within ccNSO might include policy on deployment of IDNs at the top-level and preserving universal resolvability.

The IANA function: day-to-day technical operations

The IANA functions are of foremost importance to all the ccTLD operators. A principal responsibility that ICANN has vis-à-vis the ccTLDs is that of maintaining the IANA records, while a main obligation of ccTLDs vis-à-vis ICANN is providing ICANN with information to keep the IANA records up-to-date. The Internet Assigned Numbers Authority (IANA) functions are the technical co-ordination functions of IP allocation, protocol parameter co-ordination and DNS root file management. ICANN plans to improve the IANA service that it provides to the ccTLD community as well as focus on improving outreach and engagement with the community to deliver a more efficient and responsive service.[108]

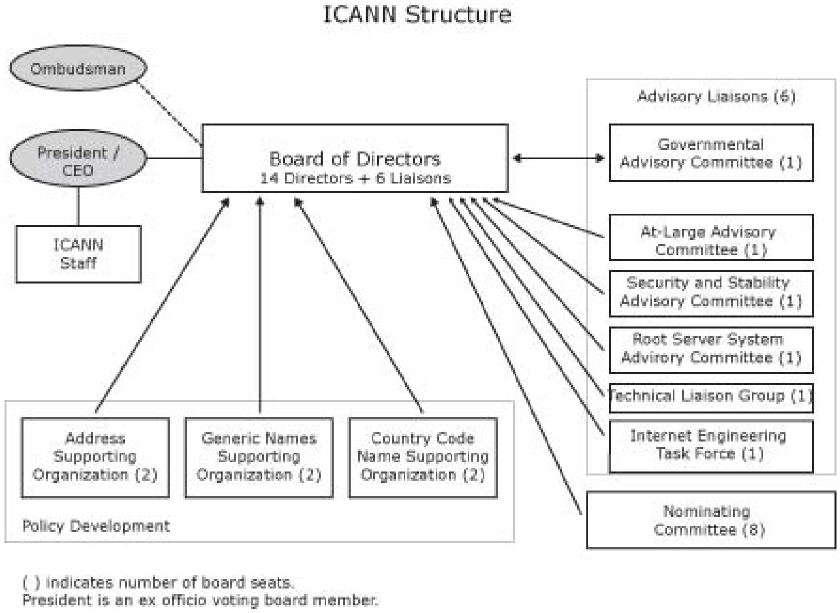
In particular, the work currently in progress within the ccNSO to formalise the relationship between ccTLDs and ICANN is deemed by some to be of high importance. The ccNSO has not, at the time of writing, passed a Charter on IANA. This involves in particular quantifying the costs to ICANN associated with the IANA functions, listing the specific IANA functions and day-to-day technical operations, as well as providing timeframes for the various operations required from ICANN. Standard functions include changing server information, upgrading to IPv6 servers or changing contact details. Each of these could benefit from a specified service level and timeframe, in order to increase the ccTLDs' level of trust. Some in the Internet community have complained that the IANA functions were not run efficiently for some time although current indications are that the situation has improved significantly recently. [109]

As a part of the IANA functions contract, ICANN receives change requests, performs controls (as the technical entity in charge of those aspects), and makes recommendations regarding them to the United States Department of Commerce, which has the operational oversight responsibility for the authoritative root zone file. All ICANN recommendations regarding top-level domain delegations, re-delegations, and name server change requests require authorisation from the United States Department of Commerce before being added to the authoritative root zone file. In its role as implementor of IANA-approved changes to the primary root name server, VeriSign additionally performs its own checks before implementation in the root zone.

"e-IANA" is a tool developed by NASK to automate many of the IANA functions, providing ccTLD managers with a greater degree of autonomy. [110] NASK, the registry of Internet names under the .PL domain, and ICANN have reached an agreement on the licensing of the NASK-developed "e-IANA" root zone management software.[111] For those registries that do not want to use the web interface, they have the possibility to appoint another trusted party to perform the updates for them.

ANNEXES

ANNEX 1. ICANN Structure, as of October 2003


ICANN Structure
Ombudsman
President / CEO
ICANN Staff
Board of Directors
14 Directors + 6 Liaisons
Advisory Liaisons (6)
Governmental Advisory Committee (1)
At-Large Advisory Committee (1)
Security and Stability Advisory Committee (1)
Root Server System Advirory Committee (1)
Technical Liaison Group (1)
Internet Engineering Task Force (1)
Nominating Committee (8)
Address Supporting Organization (2)
Generic Names Supporting Organization (2)
Country Code Name Supporting Organization (2)
Policy Development
( ) indicates number of board seats.
President is an ex officio voting board member.

Note: ICANN's Address Supporting Organization consists of the five following constituencies: ARIN, RIPE NCC, APNIC, LACNIC and AFRINIC. ICANN's Generic Names Supporting organisation includes the six following constituencies: gTLD registries, registrars, Internet Service Providers, Consumers, Academia, and Intellectual Property.

Source: http://www.icann.org/committees/nom-comm/formalcall-30jun04.htm

ANNEX 2. Number of registrations, June 2005

	Country	Counts	Date		Country	#	Date		Country	#	Date
de	Germany	8,840,396	Jun05	je	Jersey	5,000	Dec02	kn	Saint Kitts and Nevis	559	Jan02
uk	United Kingdom	4,226,097	Jun05	ac	Ascension Island	4,954	Mar03	al	Albania	500	Jun05
nl	Netherlands	1,540,799	Jun05	gt	Guatemala	4,852	Jun05	gp	Guadeloupe	500	Jun05
ar	Argentina	1,170,000	Jun05	eg	Egypt	4,467	Jun05	cu	Cuba	449	Dec03
it	Italy	1,071,046	Jun05	cr	Costa Rica	4,310	Jun05	pg	Papua New Guinea	430	Jan02
us	United States	862,090	Jun05	cy	Cyprus	4,200	Jun05	ye	Yemen	400	Jun05
br	Brazil	783,010	Jun05	vg	Virgin Islands (British)	4,200	Jun05	bh	Bahrain	380	Apr02
jp	Japan	734,520	Jun05	kz	Kazakhstan	4,092	Aug02	bw	Botswana	360	Jan02
ch	Switzerland	713,682	Jun05	bg	Bulgaria	3,952	Jun05	sc	Seychelles	353	Jan02
cn	China	622,534	Jun05	py	Paraguay	3,947	Jun05	af	Afghanistan	350	Jun05
kr	Korea, Republic of	612,644	Jun05	am	Armenia	3,930	Jun05	bd	Bangladesh	325	Dec03
dk	Denmark	607,139	Jun05	gs	South Georgia and South Sandv	3,900	Jun05	ki	Kiribati	302	Jun05
ca	Canada	553,292	Jun05	ec	Ecuador	3,581	Dec02	mq	Martinique	300	Jun05
au	Australia	551,291	Jun05	dm	Dominica	3,548	Jun05	dz	Algeria	287	Apr03
be	Belgium	438,390	Jun05	bo	Bolivia	3,500	Dec03	nr	Nauru	284	Jun05
at	Austria	428,409	Jun05	ni	Nicaragua	3,403	Jun05	aw	Aruba	275	Jun05
fr	France	376,339	Jun05	ke	Kenya	3,277	Jun05	vi	Virgin Islands (USA)	218	Aug02
ru	Russian Federation	368,320	Jun05	lk	Sri Lanka	3,200	Jan05	gf	French Guiana	200	Jun05
se	Sweden	346,419	Jun05	tm	Turkmenistan	3,079	Mar03	et	Ethiopia	190	Jun05
pl	Poland	326,566	Jun05	jm	Jamaica	3,021	Jun05	mg	Madagascar	159	Jan02
tw	Taiwan	275,788	Jun05	ky	Cayman Islands	3,000	Dec03	gy	Guyana	156	Jan02
no	Norway	236,704	Jun05	pa	Panama	3,000	Jun05	bn	Brunei Darussalam	150	Jan02
cz	Czech Republic	206,073	Jun05	sh	St. Helena	2,905	Aug02	gn	Guinea	142	Jun05
ws	Western Samoa	200,000	Jun05	mn	Mongolia	2,700	Jun05	gd	Grenada	128	Jan02
hu	Hungary	199,600	Jun05	ba	Bosnia and Herzegovina	2,605	Jun05	kh	Cambodia	119	Jan02
nz	New Zealand	191,971	Jun05	lb	Lebanon	2,584	Jun05	mr	Mauritania	106	Jan02
za	South Africa	188,259	Jun05	tt	Trinidad and Tobago	2,500	Jun05	sr	Suriname	103	Jan02
ua	Ukraine	151,050	Jun05	mt	Malta	2,494	Jun05	bt	Bhutan	95	Dec03
mx	Mexico	132,997	Jun05	ug	Uganda	2,486	Jan05	bf	Burkina Faso	84	Jan02
in	India	131,646	Jun05	vu	Vanuatu	2,450	Jan05	lc	Saint Lucia	84	Jan02
cl	Chile	125,515	Jun05	gl	Greenland	2,400	Jun05	sb	Solomon Islands	84	Jan02
fi	Finland	104,073	Jun05	ly	Libyan Arab Jamahiriya	2,292	Aug02	cm	Cameroon	79	Aug02
nu	Niue	100,000	Jun05	hn	Honduras	2,277	Jun05	gu	Guam	62	Jan02
to	Tonga	97,335	Feb03	ma	Morocco	2,243	Jan02	fk	Falkland Islands (Malvina)	56	Jun05
hk	Hong Kong	95,934	Jun05	az	Azerbaijan	2,101	Aug02	qa	Qatar	55	Jan02
es	Spain	94,831	Jun05	nf	Norfolk Island	2,094	Jun05	cv	Cap Verde	51	Aug02
ro	Romania	93,542	Mar05	jo	Jordan	2,086	Jun05	ao	Angola	47	Jan02
sk	Slovak Republic	76,639	Jun05	bm	Bermuda	2,013	Aug02	gh	Ghana	43	Jan02
gr	Greece	75,000	June04	uz	Uzbekistan	2,013	Jan02	ne	Niger	38	Jan02
tr	Turkey	73,576	Jun05	mz	Mozambique	2,000	Jun05	lr	Liberia	34	Jun05
il	Israel	70,029	Jun05	pr	Puerto Rico	2,000	Dec03	zm	Zambia	31	Jan02
ph	Philippines	70,000	Jan05	tz	Tanzania	1,834	Jun05	ga	Gabon	28	Jan02
pt	Portugal	63,749	Jun05	tf	French Southern Territories	1,591	Oct03	io	British Indian Ocean Territory	28	Jan02
my	Malaysia	61,458	Jun05	mo	Macau	1,584	Jun05	bj	Benin	24	Jan02
sg	Singapore	52,525	Jun05	fj	Fiji	1,519	Jun05	ml	Mali	16	Jan02
ie	Ireland	48,564	Jun05	gi	Gibraltar	1,500	Jun05	td	Chad	16	Jan02
si	Slovenia	32,000	Jun05	ps	Palestinian Territories	1,500	Jun05	er	Eritrea	15	Jan02
ve	Venezuela	31,200	Jun05	fo	Faroe Islands	1,466	Jun05	om	Oman	14	Jan02
ee	Estonia	30,000	Mar05	tj	Tajikistan	1,430	Jun05	pw	Palau	14	Jan02
yu	Yugoslavia	29,500	Jun05	bs	Bahamas	1,400	Jun05	zw	Zimbabwe	11	Jan02
as	American Samoa	28,614	Aug02	tl	Timor-Leste	1,349	Jun05	mm	Myanmar	9	Jan02
hr	Croatia/Hrvatska	27,650	Jun05	sm	San Marino	1,335	Jun05	mv	Maldives	9	Jan02
bz	Belize	27,581	Mar04	sn	Senegal	1,200	Mar03	sy	Syrian Arab Republic	9	Jan02
lt	Lithuania	26,161	Jun05	ai	Anguilla	1,159	Jan02	ls	Lesotho	8	Jan02
li	Liechtenstein	22,875	Jun05	by	Belarus	1,144	Aug02	sl	Sierra Leone	8	Jan02
id	Indonesia	21,640	Jun05	kw	Kuwait	1,110	Jun05	mp	Northern Mariana Islands	6	Jan02
lu	Luxembourg	21,059	Jun05	ci	Cote d'Ivoire	1,100	Jun05	gq	Equatorial Guinea	5	Jan02
lv	Latvia	20,000	Jun05	mc	Monaco	1,048	Jan05	tk	Tokelau	4	Jan02
th	Thailand	18,583	Jun05	ck	Cook Islands	1,037	Jun05	km	Comoros	3	Jan02
ir	Iran (Islamic Republic of)	18,000	Jun05	cf	Central African Republic	1,019	Jan02	so	Somalia	3	Jan02
mu	Mauritius	14,793	Jun05	im	Isle of Man	1,000	Dec03	gw	Guinea	2	Jan02
co	Colombia	13,276	Jun05	vc	Saint Vincent and the Grenadin	1,000	Jun05	va	Holy See (City Vatican State)	2	Jan02
is	Iceland	12,300	Jun05	ad	Andorra	994	Jun05	aq	Antarctica	1	Jan02
pe	Peru	12,273	Jun05	mw	Malawi	991	Aug02	bv	Bouvet Island	1	Jan02
ae	United Arab Emirates	12,000	Dec02	ng	Nigeria	981	Jun05	sd	Sudan	1	Jan02
md	Moldova, Republic of	11,705	Jan02	dj	Djibouti	955	Aug02	sj	Svalbard and Jan Mayen Islanc	1	Jan02
vn	Vietnam	10,829	Jun05	nc	New Caledonia	930	Jun05	um	US Minor Outlying Islands	1	Jan02
ag	Antigua and Barbuda	10,000	Dec02	pn	Pitcairn Island	923	Jun05	cc	Cocos (Keeling) Islands	-	nodata
uy	Uruguay	9,382	Jun05	ge	Georgia	867	Aug02	eh	Western Sahara	-	nodata
pk	Pakistan	8,325	Mar03	kg	Kyrgyzstan	857	Jan02	hm	Heard and McDonald Islands	-	nodata
sa	Saudi Arabia	7,942	Jun05	gm	Gambia	850	Jun05	iq	Iraq	-	nodata
la	Lao People's Dem. Rep.	7,200	Jun05	pf	French Polynesia	850	Jun05	kp	Korea, DPR	-	nodata
ms	Montserrat	7,200	Jun05	cd	Congo, Dem. Rep.	824	Jan02	mh	Marshall Islands	-	nodata
mk	Macedonia, ex-Yugoslav Rep.	7,176	Jun05	tp	East Timor	813	Jan02	pm	St. Pierre and Miquelon	-	nodata
sv	El Salvador	7,087	Jun05	ht	Haiti	750	Jun05	tv	Tuvalu	-	nodata
st	Sao Tome and Principe	7,000	Jun05	rw	Rwanda	746	Jan02	sz	Swaziland	-	nodata
np	Nepal	6,200	Jan05	bb	Barbados	700	Jan04	tg	Togo	-	nodata
cx	Christmas Island	5,790	Jun05	na	Namibia	694	Jan02	tn	Tunisia	-	nodata
fm	Micronesia, Federal State of	5,400	Jun05	re	Reunion Island	687	Jun05	wf	Wallis and Futuna Islands	-	nodata
tc	Turks and Caicos Islands	5,400	Jun05	bi	Burundi	654	Jan02	yt	Mayotte	-	nodata
do	Dominican Republic	5,345	Jun05	cg	Congo, Republic of	654	Jan02				
gg	Guernsey	5,000	Dec02	an	Netherlands Antilles	576	Apr05				

Source: ZookNIC, www.zooknic.com

ACRONYMS/ABBREVIATIONS TECHNICAL TERMS/PROTOCOLS

ccTLD	Country code top-level domain name
ccTLD Registry	An entity that is responsible for administering and operating a ccTLD
DNS	Domain Name System (see RFCs 1034, 1035 and 2181)
DNSSEC	Short for DNS Security Extensions
gTLD	Generic Top-level Domain name
IANA	Internet Assigned Numbers Authority functions
ICT	Information and Communication Technology
IP address	Internet Protocol Address
ISP	Internet Service Provider
Land rush	The public launch of a new top-level domain
LIC	Local Internet Community - the Internet industry, Internet users, governmental and other public authorities of the country or territory with which the ccTLD is associated. The definition of the local Internet community may vary from one country/territory to another[112]
LIRs	Local Internet Registries
NIC	Network Information Center
Registrant	A company, organisation or individual for whom a domain name under the TLD has been registered with the TLD registry.
Registry data	Data held in the register database maintained by the ccTLD registry
RFC	Request For Comments – this document series is a set of technical and organizational notes about the Internet (originally the ARPANET), beginning in 1969, published at www.ietf.org/iesg/1rfc_index.txt
SLD	Second-level Domain name (*e.g.* .co in sony.co.jp)
TCP/IP	Transmission Control Protocol /Internet Protocol
TLD	Top-Level Domain (*e.g.* .com), the last label on the right of a domain name
Whois	A protocol to query a registry's database for information about domain name registrations.
WWW	World Wide Web
Zone file	Content included in the registry zone files include a list of the domain names that are registered in the zone (*e.g.* "oecd.org"), the names of nameservers (*e.g.* "ns1.oecd.com"), the IP Addresses of the Nameservers (*e.g.* "192.3.55.2") and timer Information (*e.g.* '86400' seconds).

ACRONYMS/ABBREVIATIONS
ORGANISATIONS

ACALAN	*Académie Africaine des Langues*
AfriNIC	African Network Information Center
APNIC	Asia Pacific Network Information Center
CENTR	Council of European National Top-Level Domain Registries
CDNC	Chinese Domain Name Consortium
DoC	U.S. Department of Commerce
EuroLINC	European Languages Internet Conference
IAB	Internet Architecture Board (previously Internet Advisory Board)
ICANN	Internet Corporation for Assigned Names and Numbers
ICANN ALAC	At Large Advisory Committee
ICANN ASO	Address Supporting Organization
ICANN ccNSO	country code Name Supporting Organization
ICANN GAC	Governmental Advisory Committee
ICANN gNSO	generic Name Supporting Organization
ICANN RSSAC	Root Server System Advisory Committee
ICANN TLG	Technical Liaison Group
ICANN-UDRP	Uniform Dispute Resolution Policy (for domain names rights)
ICCP	OECD Committee for Information, Computer and Communications Policy
IETF	Internet Engineering Task Force
INFITT	International Forum for Information Technology in Tamil
InterNIC	Internet Network Information Center
ISOC	Internet Society
ITU	International Telecommunication Union
JDNA	Japanese Domain Names Association
JET	Joint Engineering Team
MINC	Multilingual Internet Names Consortium, formed in June 2000
NIC	Network Information Center
OECD	Organisation for Economic Co-operation and Development
RIPE NCC	Réseaux IP Européens – Network Control Centre
RIR	Regional Internet Registries
UNESCO	United Nations Educational, Scientific and Cultural Organization
WIPO	World Intellectual Property Organization
WSIS	World Summit on the Information Society

NOTES

[1] Governmental Advisory Committee, GAC Communiqué – Wellington, New Zealand, 28 March 2006.

[2] A total of 93 656 202 domain names on 31 December 2005, according to ZookNIC (www.zooknic.com).

[3] April 2006 Netcraft survey, http://news.netcraft.com/archives/web_server_survey.html

[4] Resolvers are often part of the operating system or software on the user's computer.

[5] The list of ccTLDs is available at http://www.iana.org/cctld/cctld-whois.htm. Further information on its history is available at http://www.iana.org/cctld/cctld-establishment-procedures-19mar03.htm

[6] Such as in Spain for example.

[7] Loic Damilaville, Assistant CEO, AFNIC, conversation of 18 April 2006.

[8] .cat however does have a geographic identifier. ICANN is the non-profit corporation that was formed to assume responsibility for the IP address space allocation, protocol parameter assignment, domain name system management, and root server system management functions previously performed under US Government. Information on ICANN is available at http://www.icann.org

[9] ccTLDs are governed by national law because most ccTLD operators are resident in the country and thus are subject to local law.

[10] The GAC Principles and Guidelines for the delegation and administration of ccTLDs of April 2005 (http://gac.icann.org/web/home/ccTLD_Principles.rtf) update the previous principles of 23 February 2000: "1.2. The main principle is the principle of subsidiarity. ccTLD policy should be set locally, unless it can be shown that the issue has global impact and needs to be resolved in an international framework. Most of the ccTLD policy issues are local in nature and should therefore be addressed by the local Internet Community, according to national law".

[11] More control on names registered often implies human intervention and judgment, and associated delays.

[12] In many cases ccTLD registries are subject to several regulations of the country or the region in which they are based, for example regarding privacy issues related to Whois or registry liability.

[13] The revised GAC Principles and Guidelines for the Delegation and Administration of Country Code Top Level Domains were approved in April 2005 (http://gac.icann.org).

[14] DNS-sec improves the security of the DNS system through authentication of published data.

[15] A widespread solution for the "zone walking" problem is not yet available.

[16] ITU-T Study Group 17 under its Question 16 on Internationalized Domain Names has been working on IDNs since 2004: http://www.itu.int/ITU-T/studygroups/com17/sg17-q16.html. ICANN has established guidelines for the introduction of IDN on the second-level of the DNS and is testing internationalised top-

level domain labels to safeguard stability and security of the DNS. ICANN announced the creation of a President's Advisory Committee for IDNs in November 2005.

[17] http://gnso.icann.org/issues/idn-tlds/issues-report-28may06.htm

[18] The intention to perform these technical tests along a specific timeline was publicly announced on 14 March 2006:. http://icann.org/topics/idn/

[19] Since 2000, ICANN has also been working with managers of ccTLDs to document their relationship with ICANN. A list of ccTLD agreements is available at: http://www.icann.org/cctlds/agreements.html

[20] Data compiled and growth rate compiled by ZookNIC in 2006 (www.zooknic.com).

[21] http://www.verisign.com/static/036316.pdf

[22] Including online advertising banners and an informational web site (www.istnogvrij.be/ www.encorelibre.be).

[23] http://www.dns.be/pdf/Pressrelease_en_20060202.pdf

[24] This number includes not only all countries, but also many territories/protectorates etc.

[25] For the list of 245 ccTLD registries, refer to http://www.iana.org/cctld/cctld-whois.htm. In addition, although .su for the former Soviet Union has been replaced by .ru for Russia and is not listed, it is still resolvable. Some registries manage several ccTLDs. February 2006, the GAC issued its "Principles and Guidelines for the Delegation and Administration of Country Code Top Level Domains", http://gac.icann.org

[26] International Telecommunication Union Resolution 102 (Rev. Marrakesh, 2002), Management of Internet domain names and addresses: http://www.itu.int/osg/spu/resolutions/2002/res102.html (...) invites Member States *i*) to participate actively in the discussions on the management of Internet domain names and addresses and notably on progress being made in pursuit of their policy objectives; *ii*). to participate in and follow the policy, operational and technical developments of the management of Internet domain names and addresses; *iii*). to increase awareness at national level among all appropriate entities, and to encourage their participation in the management of Internet domain names and addresses.

[27] http://www.isi.edu/in-notes/rfc1591.txt.

[28] 60% of the registries surveyed from CENTR's members are classified as "private", whilst 40% are "public" entities. CENTR, A-level survey, 2005: http://www.centr.org/domainwire/domainwire-3.pdf, p12. 35 registries participated in CENTR's "A-level survey", which was launched Summer 2005 and seeks to collect data on the registries' registration procedures in all different aspects. CENTR is a membership organisation. Therefore, the results of the survey reflect the responses of its members and not of the entire ccTLD community.

[29] http://www.ntia.doc.gov/ntiahome/domainname/usca/usamend0016_10252005.pdf

[30] http://www.ntia.doc.gov/ntiahome/domainname/USDNSprinciples_06302005.htm

[31] http://gac.icann.org/web/home/ccTLD_Principles.rtf. This revised statement of principles updated the GAC principles first published in 2000.

[32] They previously had to provide several documents.

[33] EC regulations (733/2002 and 874/2004).

[34] http://www.npt.no/pt_internet/eng/regulations/regulations/Regulation_on_domain_names.pdf

[35] http://ccnso.icann.org/applications/summary-approved.shtml

[36] EU is not an official ISO 3166-1 country code, but since many users of ISO 3166-1 have a practical need to encode the "eu" name, the ISO 3166/MA reserved the two-letter combination EU for the purpose of identifying the European Union within the framework of ISO 3166-1.

[37] http://www.eurid.eu/en/shared/documents/q-reports/q1-progress-report-final.pdf

[38] http://www.eurid.eu/en/shared/documents/pressreleaseVA20050322.pdf

[39] http://www.centr.org/domainwire/domainwire-4-w.pdf

[40] The EU regulations under which Eurid functions are: http://www.eurid.eu/en/shared/documents/eu-regulations/eu-regulation-733_2002.pdf

[41] EURid is looking into cases of possible warehousing by registrars and will take action against these registrars where appropriate, http://www.eurid.eu/en/shared/documents/q-reports/q1-progress-report-final.pdf. The .eu domain names were available for registration by any registrant, through any registrar, on a first-come/first-served basis, but EURid has a policy guaranteeing equivalent access of each registrar to registry resources, with no differentiation made on the basis of transaction volume, sales revenue, resource usage or other factors. Some entities are believed to have worked around these equivalent access limitations by aggregating the resources of multiple “special purpose” registrars: the more registrar accreditations a company has access to, the more transaction capacity to register names it can bring to bear on a registry.

[42] http://www.eurid.eu/en/shared/documents/published-press-releases/press-release-suspended-domain-names-final.pdf#search=%22EURid%20press%20release%2024%20july%202006%22

[43] The DNS protocol itself does not recognise any distinction between ccTLDs and other TLD.

[44] Their technical contacts are Registry Customer Service, VeriSign Global Registry Services. The administrator of .tv is the Ministry of Finance and Tourism of Tuvalu.

[45] http://cyber.law.harvard.edu/people/edelman/open-cctlds/

[46] http://www.srsplus.com/en-def-8c522473df50/en/srsplus/partners_faq_tv.shtml

[47] “On a tiny island, catchy Web name sparks a battle”, March 29, 2006, Christopher Rhoads, *The Wall Street Journal.*

[48] Ibid.

[49] http://www.educause.edu/edudomain/show_faq.asp?code=EDUELIGIBILITY. Eligibility for an .edu domain name is limited to post-secondary institutions that are institutionally accredited, *i.e.* the entire institution and not just particular programs, by agencies on the US Department of Education’s list of Nationally Recognized Accrediting Agencies. Some non-US educational institutions, such as the University of Toronto and the United Nations University, retain their registrations from an earlier, less restrictive time. Also, registrations from foreign but US-accredited educational institutions are currently being accepted.

[50] Paul Kane, Chairman, CENTR, conversation of 19 April 2006 and Sabine Dolderer, CEO, DENIC, conversation of 26 April 2006. From a technical perspective, DeNIC's registrars do not have access to the database itself, but to a high performance registration system.

[51] OECD, 1997, Internet Domain Name Allocation Policies, http://www.oecd.org/dataoecd/12/11/2091363.pdf. OECD, 2003, Comparing Domain Name Administration in OECD Countries, http://www.oecd.org/dataoecd/46/38/2505946.pdf

[52] For a more in-depth description of the mechanisms, see OECD, 2005, "The Secondary Market for Domain Names", http://www.oecd.org/dataoecd/14/45/36471569.pdf

[53] Giovanni Seppia, Global Partnership European Liaison, ICANN, conversation of 20 April 2006.

[54] OECD, 1997, "Internet Domain Name Allocation Policies", http://www.oecd.org/dataoecd/12/11/2091363.pdf. OECD, 2003, "Comparing Domain Name Administration in OECD Countries", http://www.oecd.org/dataoecd/46/38/2505946.pdf.

[55] CENTR, A-level survey, 2005, http://www.centr.org/domainwire/domainwire-3.pdf, p12. 35 registries participated in CENTR's "A-level survey", which was launched Summer 2005 and seeks to collect data on all different aspects of the registries' registration procedures.

[56] The "Canadian Presence Requirements For Registrants" policy document is available at: http://www.cira.ca/en/documents/q3/CanadianPresenceRequirementsForRegistrants-EffectiveDateJune52003.pdf

[57] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002R0733:EN:HTML

[58] http://arbiter.wipo.int/trademark/output.html

[59] ICANN adopted a Uniform domain name Dispute Resolution Policy (UDRP), developed in part by the World Intellectual Property Organisation (WIPO), to resolve domain names disputes, in particular issues relating to cyber-squatting, before a registrar cancels, suspends, or transfers a domain name. The reason behind this was that the speed of judicial review was inconsistent with the rate of growth of the Internet: UDRP provides a "fast-track" resolution process whereby parties can also if they wish invoke a standard judicial review process. The UDRP is applied by ICANN to accredited registrars in most generic top-level domains and sponsored TLDs, and by some managers of country code top-level domains, www.icann.org/udrp/udrp.htm

[60] Charles Shaban, Executive Director, Regional Office, Abu-Ghazaleh Intellectual Property (AGIP), conversation of 12 April 2006.

[61] Nominet's dispute resolution service policy is available at: www.nominet.org.uk/disputes/drs/policy/. CIRA's dispute resolution policy is available at: http://www.cira.ca/official-doc/CDRP_Policy_2003-12-04_en_final.pdf and its rules are available at: http://www.cira.ca/official-doc/CDRP_Rules_2003-12-04_en_final.pdf

[62] ASCII is the American Standard Code for Information Interchange. It is important that the sole implementation of IDNs at the registry level does not necessarily mean that users can type them into a browser or use them in e-mails.

[63] The world economy works using the DNS, which is stable since 1984 (RFC 920).

[64] http://www.internetworldstats.com

[65] See for instance Abdullah Daftardar, General Manager Technical Standards Communications and Information Technology Commission (CITC), Kingdom of Saudi Arabia.

[66] Experts in favour of a major overhaul included i-DNS, http://www.i-dns.net

[67] They use a client-side set of procedures and plug-ins that are implemented at the edge of the DNS within application, with the DNS itself not concerned since each application separately transcodes what it sees as Unicode from/to the user. A simplified description of the process is that Unicode strings are first “translated” into punycode, which means non-ascii characters are translated into a fully ASCII version of the original domain and "xn--" is added in the front of the resulting string. An important RFC for the IDNA standard is http://www.rfc-editor.org/rfc/rfc3490.txt

[68] ACE for ASCII Compatible Encoding.

[69] Adding “xn--" in front of the name so that it is recognised as IDN is termed ACE; or ASCII-Compatible Encoding.

[70] http://icann.org/announcements/idn-global-deployment-17nov05.pdf

[71] http://www.icann.org/topics/idn/implementation-guidelines.htm

[72] http://www.centr.org/domainwire/domainwire-4-w.pdf

[73] CENTR, A-level survey, 2005, http://www.centr.org/domainwire/domainwire-3.pdf, p12. 35 registries participated in CENTR’s “A-level survey”, which was launched Summer 2005 and seeks to collect data on the registries registration procedures in all different aspects.

[74] http://www.arabic-domains.org/ar/main-ar.php (SaudiNIC is participating in a pilot project among all members of the Arab League testing the use of Arabic language in domain names).

[75] Paul Kane, Chairman, CENTR, conversation of 19 April 2006.

[76] http://icann.org/topics/idn/

[77] http://www.icann.org/announcements/proposal-dname-equivalence-mapping-tld-12dec05.pdf

[78] http://www.rfc-editor.org/rfc/rfc3492.txt, RFC 3492, Punycode: A Bytestring encoding of Unicode for IDNA and http://www.rfc-editor.org/rfc/rfc2672.txt, RFC2672, Non-Terminal DNS Name Redirection (DNAME).

[79] Phishing is a form of criminal activity, characterised by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business. The term arises from the use of increasingly sophisticated lures to "fish" for users' financial information and passwords.

[80] http://www.circleid.com/posts/mozilla_implements_tld_whitelist_for_firefox_in_response
_to_idn_homographs_/

[81] http://www.icann.org/general/idn-guidelines-20jun03.htm

[82] http://www.icann.org/general/idn-guidelines-22feb06.htm

[83] http://www.icann.org/announcements/announcement-14mar06.htm

[84] http://gnso.icann.org/issues/idn-tlds/issues-report-28may06.htm

[85] GAC communiqué of 24 March 2006 from Professor Hualin Qian, ICANN Board member from China.

[86] The prospects for Chinese domain names: http://en.ce.cn/Insight/200607/04/t20060704_7602215.shtml

[87] CENTR, A-level survey, 2005, op. cit.

[88] Ibid.

[89] Including nameserver names and addresses as well as contact information.

[90] This option is described at: http://www.afnic.fr/outils/whois/aide#notebas1

[91] Nominet does not show e-mail addresses or phone numbers either, as further detailed at http://www.nominet.org.uk/other/whois/optout/. The opt-out option is available to individuals using domain names for personal as opposed to professional or commercial purposes.

[92] DNSSec previously listed each name in a numerical sequence of 1, 2, 3 etc. which meant that each name in the registry could be queried based on a simple numerical sequence and the zone file data could be entirely rebuilt in this way.

[93] DNSSec is used for the national top-domain .se in Sweden in a test operation, which started in September 2005.

[94] RIPE NCC is one of five Regional Internet Registries (RIRs) providing Internet resource allocations, registration services and co-ordination activities that support the operation of the Internet globally.

[95] ICANN performs the IANA functions under contract to the US Department of Commerce. See http://www.ntia.doc.gov/ntiahome/domainname/iana.htm. The IANA functions contract was amended and renewed several times.

[96] Through the NTIA. In response to proposals at the World Summit on the Information Society for international control of the domain name system, the Congress and the Senate both expressed their support for maintaining US control over ICANN in 2005. Kruger G. Lennard, Internet Domain Names: Background and Policy Issues, Congressional Research Service (CRS). March 3, 2006. http://www.ipmall.info/hosted_resources/crs/97-868_060320.pdf

[97] http://www.ntia.doc.gov/ntiahome/domainname/USDNSprinciples_06302005.htm

[98] Governmental Advisory Committee, GAC Communiqué – Wellington, New Zealand, 28 March 2006.

[99] http://www.oecd.org/dataoecd/34/9/34727842.pdf

[100] http://www.centr.org/domainwire/domainwire-4-w.pdf

[101] The GAC usually invites the whole ccTLD community rather than only ccNSO members.

[102] Since 2000, ICANN has also been working with managers of ccTLDs to document their relationship with ICANN. A list of ccTLD agreements is available at: http://www.icann.org/cctlds/agreements.html

[103] Loic Damilaville, op. cit.

[104] As of 1 September 2006, http://ccnso.icann.org/applications/summary-approved.shtml and http://ccnso.icann.org/applications/summary-new.shtml

[105] Including the two small territories of Gibraltar and the Cayman Islands. 13 are from Africa, 13 from Latin America and the Caribbean, 12 from the Asia-Pacific region, and 4 from North America.

[106] ICANN bylaws, Article IX: Country-Code Names Supporting Organization, http://www.icann.org/general/bylaws.htm#IX

[107] http://ccnso.icann.org/minutes/minutes-28mar06.pdf

[108] http://aptld.org/meeting/2006/03_Wellington/2006-03-wgtn-communique.htm

[109] Paul Kane, op.cit..

[110] The IANA is perceived as somewhat political because the role of the US Department of Commerce is to verify that the IANA processes for the functions of creating a new TLD, modifying a name server, and replacing a TLD manager have been followed (as shown at http://www.dns.pl/iana/process_definition.htm). In the case of e-IANA, NASK Poland did the actual development work.

[111] http://www.icann.org/announcements/announcement-05jul06.htm

[112] “CENTR Position”, “Best Practice Guidelines for ccTLD Registries”, 19 September 2003.