Antelope Consulting

Internet domain management for telecommunications regulators

Robert Milne
Antelope Consulting
rem@antelope.org.uk
www.antelope.org.uk
March 2006

Contents

1 Summary

1.1 Scope

This report discusses national internet domain management, taking account of work by international organisations and other regulators. It does not provide a comprehensive discussion of internet domain management but instead concentrates on matters of significance to the national internet domain manager and the telecommunications regulator, especially in developing countries. It does not take a position on matters of global internet governance: it describes what happens, irrespective of whether the current arrangements are accepted as appropriate by the international community. The suggestions throughout it are contributions to a debate more than definitive conclusions.

1.2 Synopsis

The report is structured as follows:

- The technical and institutional frameworks for national internet domain management are outlined in sections **Error! Reference source not found.** and 2.2.
- The functions of the national internet domain manager are identified in sections 3.1 and 3.2.
- Control of the national internet domain manager and related organisations is discussed in sections 4.1, 4.2, 4.3, 4.4 and 4.5. This involves maintaining oversight, encouraging competition, and developing core expertise in ways that are not always easily reconciled.
- Creating second level domains and allocating domain names are discussed in sections 5.1 and 5.2.
- Constructing domain names and resolving disputes about domain names are discussed in sections 6.1 and 6.2. These are seen as matters for consumer protection: to reduce the scope for confusing and misleading names, the approaches suggested demand rather more regulation and offer rather less flexibility than is sometimes found.
- Operating domain name servers and publishing registration information are outlined in sections 7.1 and 7.2. These are the main technical functions of the national internet domain manager but they also have effects on consumer protection.
- The tElephone NUmber Mapping (ENUM) is considered in sections **Error! Reference source not found.**, 8.2, 8.3, 8.4, 8.5 and 8.6. It creates problems like those for national internet domain management, even though it might not be handled by the national internet domain manager.

2 Background to national internet domain management

2.1 The technical framework

A domain name, such as 'bigglobalcompany.co.za', comprises a sequence of domain labels (which themselves are sequences of characters) separated by '.'. Domain names are hierarchical, with the "highest" domain label at the right and the "lowest" domain label at the left (by contrast with IP addresses and phone numbers). The "highest" domain label is the top level domain label; the second and third level domain labels are successively "lower"; for example, in 'bigglobalcompany.co.za', 'za', 'co' and 'bigglobalcompany' are respectively the top, second and third level domain labels, with the top level domain label, 'za' signifying South Africa. Figure 1 depicts this structure, along with structures underneath two other domain labels ('com' and 'int')

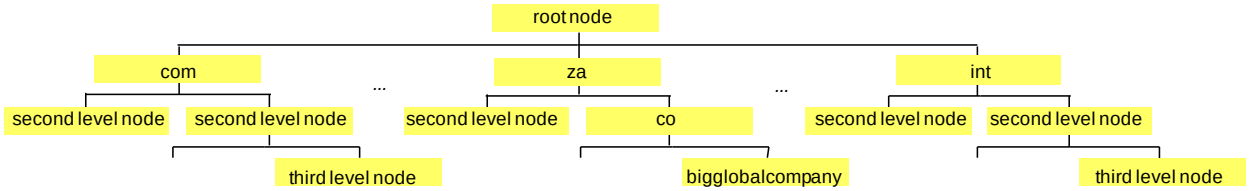

Figure 1 Structure in the 'za' domain

There are generic Top Level Domain (gTLD) labels, such as 'int' and 'com', and country code Top Level Domain (ccTLD) labels, such as 'uk' and 'za'[1]. The gTLDs and ccTLDs are not exactly as their names might suggest; for instance, 'cat' is a gTLD for the culture associated with Catalan (spoken in part of Spain) and 'eu' is a ccTLD for the countries of the European Union (EU)[2]. The gTLDs are created by the Internet Corporation for Assigned Names and Numbers (ICANN); the ccTLDs are mainly drawn from a list due to the International Organization for Standardization (ISO) and therefore have two characters each[3]. The main subject of this report, national internet domain management, is ccTLD management.

For some top level domain labels, few rules govern who may be allocated domain names; for instance, 'fr' and 'de' (which are the domain labels for France and Germany respectively), as well as 'com' and 'info', let any user have any available second level domain label for which the characters and length are allowed. For other top level domain labels, there are more rules; for instance, the 'uk' domain label for the United Kingdom (UK) is restricted to certain second level domain labels, and some of those have further restrictions (as, for example, 'plc.uk' is provided only to public limited companies), while the 'int' domain label is provided

[1] In this report the term 'domain' refers to a domain label in appropriate contexts. The term 'label' is rare outside descriptions of domain name syntax, where it is not usually accompanied by 'domain'.

[2] For the campaign leading to the creation of the 'cat' gTLD see *Cultural diversity in cyberspace: The Catalan campaign to win the new .cat top level domain* (First Monday, January 2006) at http://www.firstmonday.org/issues/issue11_1/gerrand/index.html.

[3] See *English country names and code elements* at http://www.iso.org/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html. There are very few ccTLDs that are not on the ISO 3166-1 list of two-letter codes; they are generally on an ISO reserved list of countries and groups of countries that change their names (such as the Democratic Republic of the Congo, formerly Zaire, with 'zr'), that use different codes for purposes other than the original ISO 3166-1 purposes (such as the UK, with 'uk') or that plead exceptional circumstances (such as the EU, with 'eu').

only to international treaty organisations, such as the International Telecommunication Union (ITU), which has domain name 'itu.int'. The value and nature of such rules is considered in section 6.1.

Some countries benefit commercially by having top level domain labels that make meaningful domain names when put with suitable second level domain labels[4]. However, such domain names produce not just opportunities for sales but also disputes about misuse.

The hierarchy of domain names is used in domain management, particularly in allocating domain labels and mapping domain names to IP addresses. Usually ICANN delegates the management of top level domains to specific organisations ("registries"). These organisations create, and delegate the management of, second level domains; the organisations responsible for the second level domains create, and delegate the management of, third level domains, and so on. Different organisations may therefore manage different domains. The domains which an organisation manages, together with references to the subdomains for which it has delegated management, constitute "zones".

Domain names are intended to be conveniently memorable or descriptive identifiers while IP addresses are intended for internet routing. Internet operation therefore involves mapping domain names to IP addresses. A global hierarchy of name server computers, accommodating the hierarchy of domain names, maintains the Domain Name System (DNS) that maps between domain names and IP addresses. When a message is to be sent to a domain, DNS translates the domain name into the IP address to which the message is routed. Managing a domain brings responsibility for the correct operation of the servers.

The DNS name servers for the top level domains are controlled by the registries under the guidance of ICANN. The administrative details of registration are handled by other organisations ("registrars") on behalf of users: users that wish to hold particular domain names register them with registrars, who pass information about the domain names and IP addresses to the registries for storage in the servers.

The data base that associates top level domains with their registries is maintained by the Internet Assigned Numbers Authority (IANA) on behalf of ICANN. IANA also maintains the data base of overall allocations of IP addresses. The registries for top level domains are often not involved in IP address allocation: IANA usually allocates IP addresses to Regional Internet Registries (RIRs), which then allocate IP addresses to Local Internet Registries (LIRs) such as Internet Service Providers (ISPs), which then allocate IP addresses to users.

2.2 The institutional framework

Globally, domain management is co-ordinated by ICANN. Some ccTLD managers regard themselves as having authority independent of ICANN[5]. However, in many countries ICANN is taken to be able to delegate ccTLD management to suitable organisations.

---

[4] For example, up to US$50M is being paid over twelve years to Tuvalu by an organisation that has leased the right to provide registrations of second level domain labels attached to the 'tv' top level domain label. Such rights can be revoked if ICANN finds that the registry is not acting sufficiently in the interests of the country, as happened for the 'pn' top level domain label for Pitcairn Island. Even without a deliberately commercial policy the top level domain label can appear in meaningful domain names (as with 'pep.si', which depends on the 'si' top level domain label for Slovenia).

[5] For example, at http://www.nominet.org.uk/governance/authority/ the ccTLD manager in the UK mentions the UK internet community and the UK government as sources of its authority but not ICANN. Indeed, the naming system in the UK predated DNS and originally had names the opposite way round (with 'uk.', or 'gb.', at the beginning instead of '.uk' at the end).

When delegating ccTLD management, ICANN follows principles that have been established for some years[6]. The Government Advisory Committee (GAC) of ICANN used these principles in documenting its view of the intended relations between governments, ccTLD managers and ICANN[7]. According to this view each government is responsible in its territory for developing public policy but that ICANN is responsible for the ensuring that the internet domain name system provides effective and interoperable global naming.

ICANN can redelegate ccTLD management to another organisation. However, redelegation takes some time, because ICANN must satisfy itself that the organisation can do the job well and that the stakeholders (such as the local internet community and the government) want redelegation. A ccTLD manager can contract out functions but remains ultimately responsible for ccTLD management until redelegation occurs.

The ccTLD manager can participate in ICANN policy development through the country code Names Supporting Organisation (ccNSO). Other international organisations might also be relevant. For instance, in Africa, African Top Level Domains (AfTLD) acts as a focal point for ccTLD management; however, it does not have powers delegated to it by ICANN and does not relate formally to ccNSO[8].

ICANN expects the ccTLD manager to operate the domain name servers effectively, meeting at least the criteria listed in section 7.1. ICANN also notes that ccTLD managers are trustees of their ccTLDs for their countries and the global internet community with a duty of treating all registrants fairly. In particular the ccTLD manager should:

- Be equitable and fair to all groups requesting domain names, specifically by processing, and applying rules to, all requests in a non-discriminatory way.
- Make available for public inspection policies and procedures for the use of the ccTLD, particularly documenting any features specific to the country.
- Treat requests from commercial and not-for-profit organisations on equal bases.
- Have no bias to requests from customers of another business (such as data network operation) related to the ccTLD manager.
- Make no stipulation requiring the use of a particular application, protocol, or product.

IP address management is performed through a different global hierarchy, in which IANA allocates IP addresses to RIRs, RIRs allocate IP addresses to LIRs and LIRs allocate IP addresses to users. The RIRs and, often, the LIRs do not have the same spans of control as the ccTLD managers: the RIRs relate to whole continents, not individual countries, and the LIRs often relate to individual service providers, not whole countries.

---

[6] See *ICP-1: Internet Domain Name System Structure and Delegation (ccTLD Administration and Delegation)* (ICANN, May 1999) at http://www.icann.org/icp/icp-1.htm.

[7] See *Principles and guidelines for the delegation and administration of country code top level domains* (GAC, April 2005) at http://gac.icann.org/web/home/ccTLD_Principles.rtf.

[8] AfTLD is one of several groups with or without formal organisations (sometimes termed 'the Af* groups') for developing internet capabilities in Africa. Others are the African Network Operators' Group (AfNOG), the African Internet Service Providers' associations' Association (AfrISPA) and the African Network Information Centre (AfriNIC). AfriNIC differs from the rest in that it does have delegated powers, as the Regional Internet Registry (RIR) for Africa.

3 Purposes of national internet domain management

3.1 The main purposes

The main roles of the ccTLD manager are:

- Developing policies and processes for:
  - The creation of subdomains.
  - The operation of subdomain registries.
  - The accreditation of registrars.
  - The registration of names in subdomains.
- Developing policies and processes for
  - The construction and allocation of names.
  - The resolution of disputes about names.
  - The publication and restriction of information about registrants.
- Managing technical operations of:
  - Primary and secondary ccTLD name servers.
  - Zone files with addressing information for the subdomains of the ccTLD.
  - Data bases to be searched for finding registrations in the ccTLD.

The policies and processes for subdomains might constrain second level domains more than third level domains. For instance, as in South Africa and the UK the ccTLD manager might have a fixed list of second level domains but allow any third level domains to be registered if they satisfied certain rules, as discussed in section 6.1.

3.2 Other potential purposes

Besides performing main roles the ccTLD manager might carry out related registration activities, such as:

- Acting on behalf of small ISPs as an LIR by allocating to the ISPs IP addresses provided by the RIR.
- Acting under delegation from the telecommunications regulator as to licence ISPs.
- Holding a register of ISPs adhering to a code of conduct.

Though the first example above, acting as an LIR, would not be counter to internet practice or government expectations, it might not be wanted by the ISPs themselves. Also, trade associations for ISPs might be interested in carrying out these activities, but they might well not have strong enough support or funding to become an industry self-regulator like that needed by the second and third examples above.

To establish effective ccTLD management can be a large enough challenge, without giving the ccTLD manager extra roles.

An effective ccTLD manager will be well equipped to provide an authoritative perspective on a national view of international problems such as internet governance.

4 Control of national internet domain management

4.1 Selecting the domain manager

In many countries the development of telecommunications can point to changing the organisation to which ccTLD management is delegated. Doing this might entail getting the agreement of the existing ccTLD manager, as ICANN can be reluctant to act when redelegation is contested by any of the organisations concerned[9]. Possible ccTLD managers include the following:

- **The original fixed network operator**. In some countries, for historical reasons the original fixed network operator provides both ISP functions and domain name registry functions; examples include Bahrain, Equatorial Guinea, the Maldives and Vanuatu. Other ISPs then sometimes fear discrimination or bias, or the exploitation of privileged knowledge of users for commercial purposes. To counter this, the ISP functions and domain name registry functions of the original fixed network operator could be separated. The registry would at least have its own web site and adopt transparent policies and processes. Ideally, the registry would have its own board (which could include representatives from the telecommunications regulator, other ISPs and users) to decide its policies and monitor and audit its processes for non-discrimination.
- **A not-for-profit enterprise**. The use of a not-for-profit enterprise as the ccTLD manager is perhaps the option with greatest appeal to ISPs. However, setting it up in this way is rarely feasible until there are strong wireline or wireless ISPs that can compete with the original fixed network operator (as in Australia, France, Germany and the UK, for example). In the absence of such competitors there can nevertheless be special circumstances in which not-for-profit enterprises become the ccTLD managers[10]. The enterprise might be closely associated with an ISP industry association (as in New Zealand) and might also have nominees of the telecommunications regulator or government ministries on its board (as in South Africa).
- **An academic institution**. The use of a suitable academic institution, such as a university or the national research and education network operator, as the ccTLD manager is still widespread in both large and small countries; for instance, it is found in Croatia, Cyprus, Fiji, Guyana, Ireland, Jamaica, Lesotho, Macau, Slovenia and Turkey. Again the reasons for this are partly historical: academic institutions had the requirements for, and expertise in, internet technology before most commercial organisations. Such organisations might well have reputations for registering domain names effectively and without discrimination or bias. Nonetheless, with the growth of the local internet community, they might ask, or be asked, to relinquish their responsibilities; overall the number of countries that use academic institutions as ccTLD managers appears to be falling.

---

[9] This is illustrated by the case of Pitcairn Island, where redelegation took four years though it was favoured by all fifty inhabitants (except, until late on, the administrative contact required by ICANN and his wife). For that case, see http://www.iana.org/reports/pn-report-11feb00.html. By contrast, in the case of Kenya, redelegation was quite speedy when it was requested formally, because for some years already the needs of the internet community had exceeded the time available from the administrative contact. For that case, see http://www.iana.org/reports/2002/ke-report-20dec02.html.

[10] For an example see http://www.iana.org/reports/2006/gs-report-07mar2006.pdf, which reports on redelegation for South Georgia and the South Sandwich Islands. There the resident population consists of scientists who have needs for internet access but not necessarily for many competing ISPs.

- **The telecommunications regulator**. The telecommunications regulator could assume formal responsibility for ccTLD management but subcontract operations (perhaps even to the original fixed network operator). Essentially this happens in Singapore (where, however, the telecommunications regulator is a government agency) This involvement of the regulator tends to be unpopular in countries with highly developed ISPs, where it is often felt that the industry can achieve good results without outside intervention. Nonetheless, when the telecommunications regulator has a board that is independent from the government (but which might report under law to the legislature) the industry can be satisfied[11].
- **A government agency**. As with the telecommunications regulator, a government ministry or other government agency could be responsible for ccTLD management; it might then subcontract operations to a body that was more obviously qualified. Essentially this happens in Italy, Malawi, Palestine and Spain, for example. This involvement, too, is not always welcomed where ISPs are highly developed. However, sometimes it is welcomed enough as a practical way of meeting the ICANN requirements for redelegation[12].
- **An existing name registry elsewhere**. An existing registry in a different country could act as the ccTLD manager. This could be appropriate for small countries: it is illustrated not only by Guadeloupe and Mayotte, both of which are closely linked to France, but also by Liechtenstein, which relies on Switzerland in this respect. Several Caribbean countries have relied on the University of Puerto Rico to provide domain name registry functions for them until their own capabilities have developed sufficiently to take over. Using an existing registry in this way gives the advantages of undoubted independence and competence, but the disadvantages of lack of local sensitivities and control.
- **A commercial enterprise**. An industry has grown up around the management of ccTLDs of small countries by commercial enterprises. Anecdotally not all governments that have chosen commercial enterprises as ccTLD managers are happy with the results, because there are difficulties in ensuring that the ccTLD is managed to the greatest possible benefit of the community. Many of the countries for which there are commercial enterprises as ccTLD managers have very small populations and consequently very small communities to serve; even then, vigilance might be needed to ensure that domain names are not used in ways out of keeping with their cultural and religious values.

Aspects of these are discussed further in sections 4.2 and 4.3.

4.2 Governing the domain manager

There are broadly the following possible arrangements for regulation:

- **Statutory regulation**. Public authorities counter abuse by exercising statutory powers.
- **Co-regulation**. Public authorities and industry participants collectively counter abuse by exercising statutory powers if private action and informal coercion fail.
- **Self-regulation**. Industry participants collectively counter abuse by exercising private action and informal coercion.
- **No regulation**. Industry participants individually counter abuse if they are able and willing.

---

[11] For an example see http://www.iana.org/reports/2003/ky-report-30jun03.html, which reports on redelegation for the Cayman Islands.

[12] For an example see http://www.iana.org/reports/2003/af-report-08jan2003.html, which reports on redelegation for Afghanistan.

There are many ways in which these arrangements can vary; for instance, co-regulation is often distinguished from self-regulation partly because in co-regulation public authorities are likely to be represented on the boards of the regulatory organisations, and self-regulation is sometimes authorised under powers that allow the telecommunications regulator to take over if self-regulation fails completely.

Some countries lay down principles that regulators, co-regulators and self-regulators are advised to follow[13]. Often government ministries, not regulators, are responsible for monitoring adherence to the principles and auditing implementation of the principles. However, the board of the ccTLD manager could itself perform or at least initiate these monitoring and auditing functions, by noting best practice guidelines of the Council of European National Top-Level Domain registries (CENTR)[14].

Of particular concern is the extent to which co-regulators and self-regulators take account of opinions from outside their industries. Representation on the board from consumer groups can help with this. Even if there is no such representation, consultations by the ccTLD manager should be addressed to the whole community, not just to ISPs, and avoid unnecessary specialised or unexplained terminology.

In individual disputes, as well as in general policies, co-regulators and self-regulators are in danger of appearing to be serving their industries, not their consumers. In particular, domain name disputes may well pitch individual consumers against ISPs or large organisations that fund the ccTLD manager. When this is so, the ccTLD manager may well choose to contract out the function of resolving domain name disputes to independent external individuals or organisations, as discussed in section 6.2.

The adoption of policies and processes that take full account of public consultations and the use of independent outsiders for dispute resolution can do much to allay concern about the impartiality of co-regulators and self-regulators.

4.3 Relating other organisations to the domain manager

The telecommunications regulator in a country is frequently given responsibility under a communications act for the national numbering plan. The national numbering plan covers many of the numbers that are used in making calls and sending text messages; it sometimes covers all of these “numbers”, including those that contain ‘#’ or ‘*’ as well as digits. Whether the numbering plan goes beyond that, to include domain names, and whether the telecommunications regulator is the ccTLD manager, depends on the country. Often the telecommunications regulator is not the ccTLD manager, for such reasons as:

---

[13] For the example of the principles put forward in Uganda, see *Principles of Good Regulation* at http://www.goodregulation.or.ug/principles.php. For a discussion of the relation between regulation and economic development see *Doing Business in 2005: Removing Obstacles to Growth* (World Bank, 2005) at http://rru.worldbank.org/Documents/DoingBusiness/DB-2005-Overview.pdf. For a report on regulatory impact assessments in developing countries see *Regulatory Impact Assessment in Developing and Transition Economies: a Survey of Current Practice and Recommendations for Further Development* (University of Manchester, November 2003) at http://www.competition-regulation.org.uk/conferences/mcrria03/conf3.pdf.

[14] For these guidelines see *Best Practice Guidelines for ccTLD Registries* (CENTR, September 2003) at http://www.centr.org/docs/2003/09/bestpractice-guidelines.html. Despite its name, CENTR has among its forty-two members Afghanistan, Armenia, Canada, Iran, Israel and Palestine. Its counterparts in other regions of the world, such as AfTLD, have not issued corresponding guidelines.

- Registering domain names is associated with operating domain name servers. There is no real counterpart to this for numbering management; telecommunications regulators, who are intended to supervise the commercial practices of network operators, are not well suited to operating network equipment themselves. The centralised real-time data bases required in some implementations of number portability are typically operated by neutral third parties, not by the regulators[15].
- The problems of national numbers and domain names are quite different. The supply of national numbers might be inadequate or skewed to particular companies (such as large mobile service providers); subscribers wish to hold numbers but have relatively little interest in what these numbers are[16]. The supply of domain names is plentiful but coveted, but subscribers require that they, and only they, hold domain names resembling their business names or descriptions. In fact numbering management by the regulator of telecommunications has more in common with IP address management than with domain management.

The ccTLD manager is frequently a non-governmental organisation[17]. It might well have some government involvement through its board, which determines (or at least recommends) policies and processes. The board might therefore include representatives of the telecommunications regulator and appropriate government ministries. Representation of the telecommunications regulator should help to ensure consistency between policies for number management and for domain management in areas of convergence such as privacy for tElephone NUmber Mapping (ENUM). The board might also include representatives of properly organised and clearly independent consumer groups.

The ccTLD manager could contract out some functions without necessarily contracting out the aspects of ccTLD management that are more dependent on overall policies. In particular, the ccTLD manager could contract out operating the ccTLD name servers, for the national portion of the global Domain Name System (DNS). It might even need to do so, because having the servers in the country itself (as preferred by ICANN) might not be feasible without a cost-effective internet exchange in the country. Other examples of delegation by the ccTLD manager are given in section 4.4.

There might be other national organisations with powers relating to the internet. In particular, there might be organisations concerned with eliminating certain internet content, such as spam and child pornography. Again these might be non-government organisations; they might have government involvement through their boards, but they would generally prefer not to do so, to preserve as much freedom of expression as possible. Their activities (such as blocking spam or taking down child pornography in response to requests from the police) have little relation to those of the ccTLD manager, and they can be kept separate.

---

[15] The same is true for internet exchanges and for the centralised real-time data bases of ENUM.

[16] Some subscribers are interested in holding particularly memorable or otherwise desirable numbers ("golden numbers"). However, this is not the predominant problem for numbering management.

[17] An international survey in 2003 found that, among 66 countries replying to a questionnaire from ITU, 41% of ccTLD managers were not-for-profit organisations, 20% were commercial organisations, 20% were academic institutions or individuals, and 13% were public institutions. For this survey, see *Governments and Country-Code Top Level Domains: a Global Survey* (University of Ottawa, February 2004) at http://michaelgeist.ca/resc/Governments And Country-Code Top Level Domains (V.2).pdf. A slightly earlier version of this survey had been criticised on various grounds, such as that some large non-governmental ccTLD managers were missing from its numbers. For the criticism, see *Some comments on Professor Michael Geist's "Government and country-code top level Domains: A global survey"* (CENTR, January 2004) at http://www.centr.org/docs/2004/01/geistsurvey-response.pdf.

4.4 Delegating from the domain manager

The ccTLD manager may choose to delegate tasks to other organisations, while retaining ultimate responsibility. The organisations to which delegation is most likely are as follows:

- **Moderated domain managers**. Even if registrants are not allowed to register new second level domain names, second level domains, like third level domains, might themselves be managed by organisations other than the ccTLD manager, under delegation from the ccTLD manager (and with adherence to policies laid down by the ccTLD manager). In particular, this might be done for domains that allow only some registrants (such as government bodies with the 'gov' domain label). Such domains are sometimes said to be "moderated". They have their own rules about who can register subdomains within them and, occasionally, about what the names of such domains must look like. When different second level domains cater for different classes of registrant, giving them different managers does not introduce competition but loses economies of scale.
- **Registry operators**. Subcontracting certain functions of the ccTLD manager to two or more distinct registry operators (dealing with separate second level domains) would introduce competition. Even so, keeping the scarce expertise in a single pool, in just one registry operator, might be preferable. The CENTR best practice guidelines and the ICANN model ccTLD sponsorship agreement could be helpful in designing such forms of delegation or subcontract[18].
- **Registrars**. Though registrars are likely to be ISPs, they might be subject to conditions to which ISPs in general were not subject. In particular, the ccTLD manager might require registrars to perform duties on its behalf, such as:
  - Informing registrants about the ccTLD dispute resolution policy and process, perhaps by introducing contracts between the registrants and the ccTLD manager.
  - Checking that new domain names obeyed the rules outlined in section 6.1 (including those that are not easily automated).
  - Operating secondary domain name servers.

4.5 Funding the domain manager

The main day-to-day functions for which the ccTLD manager (mentioned in section 3.1) is responsible could each be self-financing are. For instance:

- Administering domain registration could be funded by charges on registrants.
- Resolving domain name disputes could be funded by charges on disputants.
- Operating domain name servers could be funded by contributions from ISPs (probably in proportion to their numbers of customers).

However, this doing this would weigh heavily on the individuals registering names or disputing rights to names. It would also not cater for activities such as participation in formulating national and international policies on domain names, or offering free name registration or dispute resolution to charities. Contributions from ISPs and, if necessary, the government should be used to subsidise the functions of the ccTLD manager to avoid excessive costs for individuals.

---

[18] For this agreement see *Model ccTLD Sponsorship Agreement* (ICANN, January 2002) at http://www.icann.org/cctlds/model-tscsa-31jan02.htm.

In principle the ccTLD manager could wish to charge higher fees for allocating especially memorable or otherwise desirable domain names. Overall the complication of doing this appears to be unjustified, for reasons mentioned in section 5.2.

A ccTLD manager that is a not-for-profit enterprise might well accrue surplus funds that can be donated to a charity. Some ccTLD managers (in Australia and the UK, for example) have set up special charities for the purpose, typically with objectives that include furthering the safe, informed and constructive use of the internet.

5 Supply of domain names

5.1 Creating second level domains

In several countries registrants can register only third level domains (in existing second level domains). The published policies and processes for creating new second level domains are needed rarely. This is so, for example, in Australia, Ghana, Kenya, Mexico, New Zealand, South Africa and the United Kingdom (UK), which have respectively 10, 5, 6, 5, 12, 16 and 13 second level domains[19]. Among the second level domain labels are usually variants of:

- 'ac' (academic institutions).
- 'co' (commercial organisations).
- 'gov' (government bodies).
- 'net' (internet organisations).
- 'org' (not-for-profit organisations).

In such countries registrations in the second level domain for commercial organisations typically predominate. Figure 2 demonstrates how dominant 'co.nz' is in New Zealand[20]. In the UK it is even more dominant: 92% of new third level domain registrations are in 'co.uk', while very few are in 'ltd.uk' and almost none are in 'plc.uk', which are alternatives to 'co.uk' for registered companies.

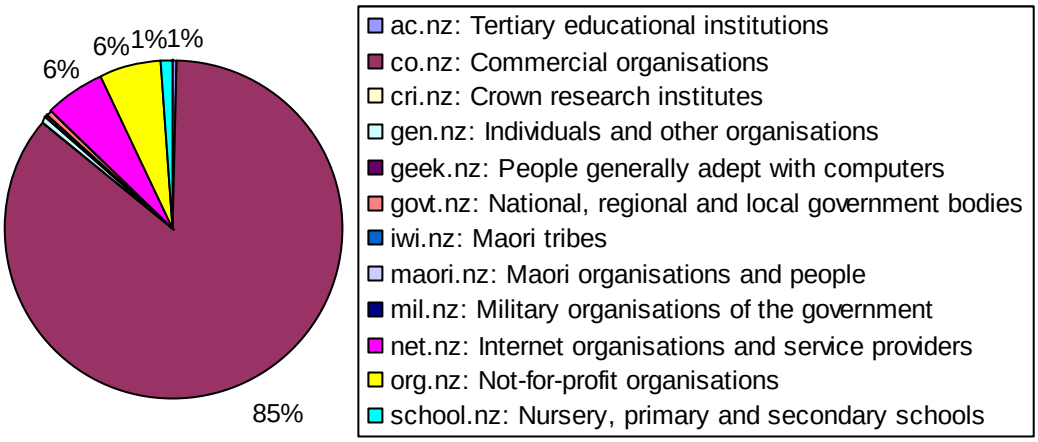

Figure 2 Proportions of names in different second level domains in New Zealand, 2005

[19] Australia has also second level domains for geographic areas corresponding to its 8 states and territories. Ghana and South Africa used to allow registrants to register new second level domains.

[20] For the basis for this figure see *.nz Statistics - by Calendar Year* at http://dnc.org.nz/content//calendar_stats.html. For related information for the UK, see *Registrations Archive* at http://www.nominet.org.uk/intelligence/statistics/registration/registrationsarchive/.

In other countries (such as Armenia, Chile, Italy, France, Germany and the Netherlands) registrants do not use existing second level domains but instead register new second level domains[21].

In yet further countries (such as Canada, Hong Kong, Japan, Palestine, Singapore and South Korea) registrants can either register new third level domains (in existing second level domains) or register new second level domains. Often the existing second level domains were introduced well before registering new second level domains was allowed. Where both registering new third level domains and registering new second level domains are allowed, new second level domains tend to be favoured (at least if the fees involved are comparable). Figure 3 shows that in Japan registering new second level domains has been much more popular than registering new third level domains since 2001, when it was first allowed[22]. This is so even if only the names using English characters, not Japanese characters, are considered.

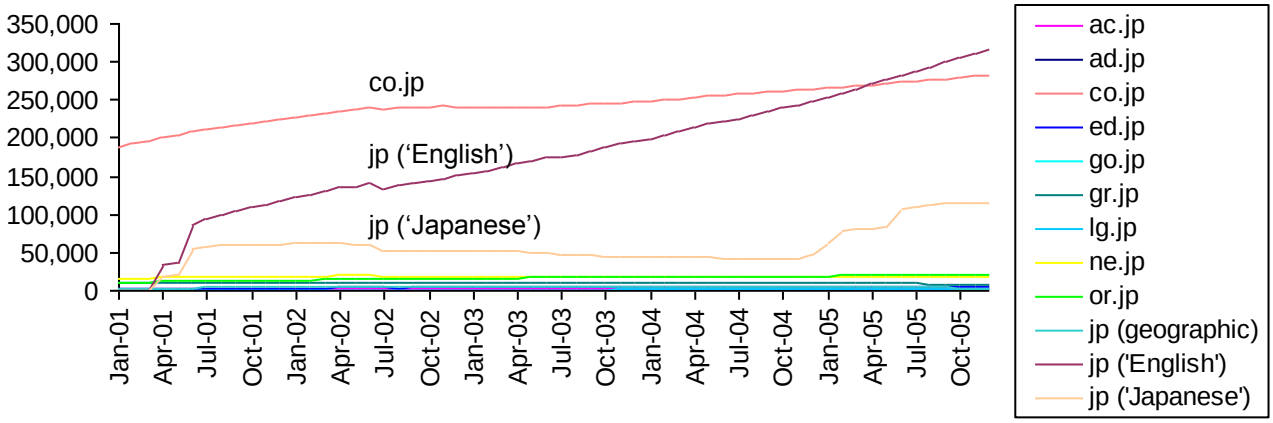

Figure 3 Growth in names in top level and second level domains in Japan, 2001-2005

Decisions about which second level domains to provide are not always just the responsibility of the ccTLD manager: they can involve larger national considerations, especially if registrants are allowed to register new second level domains. Arguments for allowing registrants to register new second level domains are:

- It might help to elevate the ccTLD to the status of 'com' inside the country, because, for example, 'bigglobalcompany.za' would look very similar to 'bigglobalcompany.com'. This might, however, add to the confusion already created by 'com', 'biz', 'info' and the rest.
- It provides equality of treatment to businesses if competitors have registered such second level domains under earlier dispensations[23].

[21] The Netherlands allows also third level domains for personal names in second level domains having numbers as labels.

[22] Japan had already second level domains for geographic areas before 2001. For further details, see *JP Domain Name Registry Report 2005* (Japan Registry Services, March 2006) at http://jprs.co.jp/en/pdf/registry-report-2005-e.pdf.

[23] For example, in Botswana the incumbent fixed network operator and its ISP have their own second level domains. Rather than letting their competitors have second level domains also, with all the attendant difficulties of deciding what constitutes a competitor, other ISPs might prefer the incumbent fixed network operator and its ISP to be relocated to the 'co.bw' or 'net.bw' second level domain.

- It does not create worse conflicts than occur in countries where only third level domains can be registered, because in those countries one particular second level domain is used predominantly, almost to the exclusion of others.
- It does not put pressure on second level domains to broaden their scopes, whilst, in countries where only third level domains can be registered, commercial organisations sometimes register with 'org', for example, because their favoured labels under 'co' are already taken by others.
- It could exploit the similarity of the top level domain name to an English suffix or abbreviation, or make available especially valuable second level domain names, by requiring high fees for some registrations[24].

If possible, the decision about whether to allow registrants to register new second level domains should be made before registration becomes widespread. Otherwise, there could be confusion unless all domain names in the ccTLD and with second level domain label 'co' are automatically made synonymous with their counterparts in the ccTLD but without the second level domain label 'co'.

If registrants are allowed to register new second level domains, then if possible there should be a 'sunrise' procedure for allocation, along the lines described in section 5.2.

5.2 Allocating domain names

Typically domain managers register names on a 'first come, first served' basis: a registrant is allocated a name after the domain manager has checked its availability and validity and has received a standard fee. The fee is essentially independent of the name and represents an administrative charge, not the value of the name to the registrant. The registrant may register more than one name. The same practices are usually followed for company name registration and trade mark registration.

However, domain names can have great value to registrants, because they may describe the goods or services of the registrants or of companies willing to buy the names from the registrants. Thus registrants can profit by making far-sighted, rapid, accidental or bulk registrations. The ccTLD manager could seek to eliminate this profit, or exploit it for defraying the costs of domain management, by using one of the following schemes:

- **Prohibition of transfers**. The ccTLD manager could prohibit transfers of names from initial registrants to other people. Doing this would eliminate the profits from name resale but be very inflexible: companies entering new markets would lose ways of acquiring the domain names that best fitted them. It would also perpetuate the advantage of registrants over their less fortunate competitors, as those competitors would be unable to acquire the names and might even be unable to register other useful names that the initial registrants had registered without necessarily intending to use.
- **Auction of names**. The ccTLD manager could guess which names were likely to be popular and seek to auction them. However, doing this would entail releasing names on the market in a controlled manner, which would inhibit internet development and be extremely irritating for people who wanted names that had not yet been released.

[24] The best known example of a domain name used in this way is 'tv' for Tuvalu, but others, such as 'am' for Armenia, 'st' for San Tomé, 'tm' for Turkmenistan, 'to' for Tonga and 'it' for Italy, are also used in this way. As a further example, Nigeria, which has ccTLD 'ng', could choose to permit such names as 'traini.ng' or 'train.i.ng'. Incidentally, names analogous to 'train.i.ng' would be avoided in many top level domains by rules on the minimum lengths of second level domain names.

- **Taxation of transfers**. The ccTLD manager could charge registrants an administrative fee for new registrations but tax registrants when names are transferred between registrants at profit. However, registrants could avoid paying the tax by using name forwarding arrangements instead of transfers.

Charging just an administrative fee both for new registrations and for transferred registrations is simplest and probably no more disadvantageous overall than the other schemes.

Domain names that are no longer needed by their original registrants should be recycled, as other people might use them more effectively. Registrations should therefore be subject to renewal (perhaps every two years) and the ccTLD manager should charge an administrative fee for renewed registrations as well as for new registrations.

Sometimes a new domain name space becomes available, because, for instance, a new second level domain is created or businesses are newly allowed to register for second level domains. In this situation the domain manager may make the space available in a phased manner, giving preferential treatment to ever broader classes of applicants in successive phases. In the last phase all applicants are admitted and all remaining names are allocated on a 'first come, first served basis'. In the earlier phases the applicants and the available names may be limited and the names are allocated randomly at the ends of the phases. For instance, with 'eu' for the EU, in the first phase (the 'sunrise' period) only trade mark holders are admitted, and in a middle phase organisations can apply for names if they have documented but possibly unregistered rights to names[25].

[25] The 'land grab' period is typically one of the phases in which all organisations may apply for names; the names available may be limited to specific 'premium' (and often generic) names, as with 'info', or unlimited, as with 'pk' for Pakistan. For the allocation process for the 'info' top level domain see *INFO Rollout Schedule* at http://www.afilias.info/register/schedule/.

6 Protection for users of domain names

6.1 Constructing domain names

Most countries have rules about the syntax of names that deal with the allowed characters and lengths, for example. These rules largely depend on, or originated from, the capabilities of the domain name servers and are not discussed much further here.

Many countries also have rules about the implicit or explicit meanings of names. These rules are more directly related to policy and are the ones mainly discussed in this section. Defining them precisely and applying them strictly could be labour-intensive but would strengthen user protection; having them without doting this could weaken user protection, by giving users a false sense of security. For these reasons the rules deserve to be considered very seriously, before the lax definition or application of them pollutes the domain name space to an extent that makes them unhelpful.

6.1.1 General rules

Registrants are usually expected to obey restrictions on what kinds of organisation have what kinds of domain name. However, often the restrictions are not enforced. Enforcing the restrictions reduces the speed and level of automation of registration, because typically paper credentials have to be submitted and validated. However, not enforcing them opens the way to confusing and misleading people. In general there is a trade-off between making registration easy and safeguarding the integrity of the domain by checking domain names.

Initially the integrity of the domain might be more important than ease of registration: especially in a country where advance fee frauds are widespread, the ccTLD must be seen to have the highest integrity for the internet community to develop confidence in it. In such cases, tight rules on registration can give people some confidence in the meanings of names. Such rules offer just some protection, not absolute defence, but they can prevent many mistakes by eliminating some potentially confusing or misleading names. Possible rules are:

- A domain name should obey rules at last as strict as those applied in the company name registry, including, in particular, rules governing the use of 'reserved' words[26]. These rules might, for example, define which classes of organisations were entitled to use words like 'bank', 'government', 'limited' or 'national' in their names.
- A second or third level domain label should not be very similar to, or be a homograph of, any top level domain label or any other second or third level domain label in the ccTLD[27]. Requiring this should not only reduce the risk of confusing or misleading people but should also ensure that a registrant need not register more than once to protect a name (with, for instance, both ''bigglobalcompany.co.za' and ''bigglobalcompany.org.za').

[26] For the list of reserved words in Hong Kong, see https://www.hkdnr.hk/eng/reservedlist/index.html.

[27] In this report the term 'very similar to' relates to names that are identical except for the possible presence of some characters (such as '-') and the possible use of some abbreviations (such as '&' for 'and'). A 'homograph' is a text written similarly to another text; thus in English two texts might be homographs if they differed only because one used a lower case 'l' and the other used an upper case 'I'. Unfortunately the notion of homograph is script-dependent (because of '0' and 'O, '1' and 'l', or '5' and 'S', for example) but the important cases could be codified for these rules.

- A third level domain label should not contain multiple character sets for Internationalized Domain Names (IDNs). Requiring this should again reduce the risk of 'phishing'[28]. In fact initially there might be no IDNs, to speed up the development and refinement of the rules for domain name construction and dispute resolution.

These rules are stated quite generally. However, they could probably be relaxed, by being applied only to commercial organisations, if accompanied by the more specific rules given in the rest of the section.

6.1.2 Specific rules for commercial organisations

To maintain the quality of the registrations of commercial organisations it is desirable that:

- The domain names of commercial organisations should be composed from parts of the company names registered for the organisations.

The company name registry in the country is often automated enough to justify requiring domain labels for commercial organisations to be very similar to company names.

When domain names are being registered, the domain managers check that names are not registered already. However, some domain managers deliberately do not check whether others might have rights in the names, particularly through trade marks. The obstacles to checking trade marks are:

- Domain managers may be legally liable to registrants and trade mark holders for errors or omissions in checks of the trade marks registry.
- Checks, particularly when they involve subjective judgements, make registration slower and dearer.
- Trade marks look very different from domain names, so deciding when they are similar is contentious and even subjective.
- Trade marks are registered for particular classes of goods or services, so holders of trade marks for different classes might have similar claims to a name.

However, other domain managers do check trade marks; Pakistan (with 'pk') and the EU (with 'eu') provide recent examples. They get around the last two of the obstacles above in the following ways:

- They avoid subjectivity by requiring that domain labels be very similar to the textual part of the corresponding trade marks.
- They give equal opportunities to trade mark holders for different classes of goods or services by allocating the names randomly among the applicants at the ends of 'sunrise' periods; after the ends of the 'sunrise' periods other names can be allocated in 'land grabs', on a 'first come, first served' basis.

Unfortunately, introducing a 'sunrise' period into the allocation process delays widespread use of the ccTLD.

---

[28] Normally 'phishing' involves attempting to get sensitive information by masquerading as someone with a need for such information. It can involve directing users to a fraudulent, but seemingly valid, web site. One domain name can look like another if it uses similar characters (such as English 'c' and Russian 'c') in the same character set or in a different character set. For the recommendation on avoiding multiple character sets see *Guidelines for the Implementation of Internationalized Domain Names* (ICANN, June 2003) at http://www.icann.org/general/idn-guidelines-20jun03.htm.

6.1.3 Specific rules for not-for-profit organisations

To reduce the risk of commercial organisations from masquerading as not-for-profit organisations:

- The domain names of not-for-profit organisations should be composed from parts of their official names.

Rules like this point to providing separate second level domains for commercial organisations and for not-for-profit organisations and to not allowing registrants to create new second level domains. Registration in a particular second level domain should then guarantee that the rules for registration in that domain are satisfied. A similar guarantee could be provided by letting commercial organisations create new second level domains but not letting not-for-profit organisations do so; however, doing this would be discriminatory.

6.1.4 Specific rules for individuals

In some countries individuals as well as organisations are allowed to register domain names; for example, 'idv.hk' in Hong Kong, 'gen.nz' in New Zealand, 'nom.za' in South Africa and 'me.uk' in the UK are arranged for this purpose. As the figures in section 5.1 indicate, these arrangements do not seem very popular. Even in the UK only 2% of new third level domain name registrations are in 'me.uk'.

If individuals are allowed to register domains, it is desirable that:

- The individuals registering domains should be permanently resident in the country and have domain names composed from parts of their personal names.

Individuals, but not registered companies, can have identical names. Allocating domain names to people could use a 'sunrise' procedure (like that for allocating domain names to companies with particular trade marks). Alternatively uniqueness could be ensured by including a number in each domain name formed from a personal name (as in the Netherlands).

6.1.5 Specific rules for others

The rules suggested in this section are rather inflexible. On their own they are probably too inflexible; for example, they do not obviously allow enthusiasts to set up web sites for informal discussions of particular topics. Many ccTLD managers have much more flexible expectations about when registrations are valid.

Some flexibility could be introduced by providing a second level domain that would be open only to registrations that would be invalid in other second level domains; in particular, commercial organisations would be excluded from it. Users would need to understand clearly that this second level domain offered few guarantees. It would be given a distinctive label such as 'info', not 'co' or 'org', to help.

6.2 Resolving domain name disputes

Rules like those given in section 6.1 say what registrations could be valid. However, they do not ensure that names that have been registered validly have been registered for acceptable reasons or used in acceptable ways. Consequently there can be disputes about this. In such disputes the complainants typically seek to have the names transferred to themselves from the respondents are the registrants of the names.

Resolving domain name disputes requires both procedures for deciding between complainants and respondents and policies for determining what decisions should be made. Both are discussed, to some extent, in this section.

6.2.1 Phasing of the procedure

Often ccTLD managers avoid involvement in resolving domain name disputes, so that they can remain neutral technical organisations. An extreme approach entails just relying on the courts to resolve disputes. However, litigation is usually expensive and cumbersome; many ccTLD managers therefore have alternative dispute resolution procedures that use independent external services other than courts. These procedures are alternatives to litigation: disputants may still use the courts as well or instead, and in particular may challenge through the courts the outcomes of these procedures. The ccTLD managers do not transfer names between disputants until the alternative dispute resolution procedures, and any recourse to the courts, come to an end.

The best known alternative dispute resolution procedure for domain name disputes is that provided by the Uniform domain-name Dispute Resolution Policy (UDRP) of ICANN[29]. This is used for the ccTLDs of some small countries as well as for gTLDs such as 'com' and 'org'. The UDRP allows an arbitrator (or, at the request of one of the disputants, three arbitrators) to decide a dispute[30]. Arbitrators are chosen by, and work on behalf of, a UDRP arbitrator provider, such as the World Intellectual Property Organization (WIPO) and the National Arbitration Forum (NAF), appointed by ICANN.

Many disputes can be resolved with less formality than even this procedure needs. Hence some ccTLD managers, such as that in the UK, have adopted alternative dispute resolution procedures having up to three stages: mediation, arbitration (if the disputants fail to agree during mediation) and appeal (if a disputant is not satisfied with the outcome of the arbitration). The use of mediation before arbitration can be very effective in making dispute resolution less cumbersome: Figure 4 shows that relatively few cases may need arbitration[31].

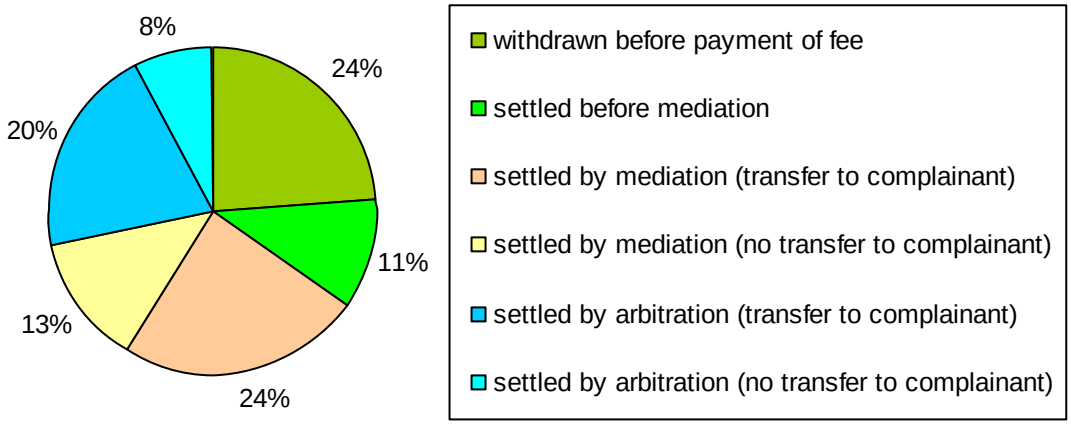

Figure 4 Outcomes of valid dispute resolution cases in the UK, 2004-2005

[29] See *Uniform Domain Name Dispute Resolution Policy* (ICANN, October 1999) at http://www.icann.org/dndr/udrp/policy.htm.

[30] In this report the term 'arbitration' is not used with any specific legal connotation. In fact the term is inappropriate in several countries because of such connotations, which suggest a much more expensive and cumbersome process than that used in name dispute resolution. The arbitration process used in name dispute resolution could be similar to that for simple disputes between customers and service providers but of course deals with a narrower range of legal questions.

[31] Almost 30% UK dispute cases are invalid for procedural reasons. Domain names are transferred to complainants in 68% of mediations and arbitrations. There are very few appeals. Over 700 cases were handled in 2004 and over 900 cases were handled in 2005. For some details, see *DRS statistics – graphical representation* at http://www.nominet.org.uk/disputes/drs/statistics/?contentId=2741.

A mediator does not make a decision but simply encourages others to reach agreement. Hence providing a mediation service would not compromise the neutrality of the ccTLD manager, which might be able to do this more cheaply than an external organisation.

However, arbitration and appeal may call for more obvious independence from the ccTLD manager. To demonstrate impartiality the ccTLD manager can appoint independent external individuals or organisations to provide arbitration and appeal services, with agreed service levels (such as numbers of cases to be handled and time to be spent per case). These individuals or organisations can be either inside or outside the country. The ccTLD manager can even adopt the UDRP and rely on the UDRP arbitrator providers appointed by ICANN. However, the procedure of the UDRP is less satisfactory than some of its successors, according to various commentators[32].

6.2.2 Interactions between the policy and the procedure

An alternative dispute resolution procedure is accompanied by a policy, which is also determined by the domain manager. The policy describes the principles of ownership that a claimant to a disputed domain name must establish and gives examples of evidence that can be used to support or rebut claims. Broadly speaking a claimant must establish that the following conditions hold:

- The disputed domain name is similar to a name or mark in which the claimant has rights.
- The disputed domain name was acquired or is used in a way unfairly exploiting, or unfairly detrimental to, these rights.

Conditions like these are in the UDRP, but they need adaptation to take account of particular national frameworks and global experience since the development of the UDRP. For instance guidelines by WIPO on adapting the UDRP point out that[33]:

- In a country where individuals and organisations must have local presence if they are to register domain names the rights of a claimant in a name or mark might need to be established specifically for that country; brand recognition in the rest of the world would not be enough.
- A disputed domain name could be acquired in good faith but used in bad faith; the UDRP demands that the disputed domain name be both acquired in bad faith and used in bad faith (though some other policies do not do so).

The recent draft New Zealand policy gives several examples of evidence useful in supporting or rebutting claims[34]. It is based on the UK policy, which in turn is related to the UDRP.

The most significant difference between policies, or at least between arbitration decisions in different countries, is perhaps the extent to which domain name resale, by people who deliberately register domains for resale, is regarded as an honourable pursuit. Differences may also result from the treatments of generic (descriptive) domain names and of criticism web sites having names like those of the criticised companies.

---

[32] For a history of, and commentary on, the UDRP see *ICANN's "Uniform Dispute Resolution Policy" – Causes and (Partial) Cures* (Brooklyn Law Journal, volume 67, pages 608-718, 2002) at http://www.law.miami.edu/~froomkin/articles/udrp.pdf.

[33] See *ccTLD Best Practices for the Prevention and Resolution of Intellectual Property Disputes* (WIPO, June 2001) at http://arbiter.wipo.int/domains/cctld/bestpractices/bestpractices.pdf.

[34] See *Dispute Resolution Service Policy* (Domain Name Commissioner, December 2005) at http://dnc.org.nz/content//draft_DRS_policy.pdf.

However, the policies tend to leave scope for individual judgement and reliance on precedent, so systematic differences may derive mainly from the attitudes of the arbitrators and, in the case of the UDRP, the arbitrator providers who add supplementary rules to the UDRP and choose the arbitrators. The arguments deployed by arbitrators under the UDRP have tended to favour complainants, who have frequently been big businesses[35]. Giving complainants the right to choose the UDRP arbitrator providers for single-arbitrator cases might have led to "forum shopping", in which complainants choose UDRP arbitrator providers that are known to make decisions favourable to complainants[36]. This defect has been avoided in some later policies based on the UDRP, such as those in Kenya[37].

6.2.3 Staffing for the procedure

Alternative dispute resolution is often performed by people having legal backgrounds. However, in several countries lay people are accustomed to similar duties in public tribunals of various sorts and are highly valued for their contributions; for instance, there is widespread satisfaction with the UK use of lay people, as well as lawyers, in arbitrations and appeals.

In practice most cases for arbitration (as opposed to appeal) are sufficiently clear-cut that one person, rather than a panel of several people, can determine their outcomes. However, some single-arbitrator decisions under the UDRP have been criticised for being capricious, and disputants sometimes appear to prefer having three arbitrators when they believe that their cases are sound and important to them.

When a country first introduces ccTLD manager, the number and complexity of name disputes could be low initially but then rise rapidly. In these cases the ccTLD manager should proceed by:

- Laying down the dispute resolution policy and procedure.
- Providing for mediation as well as arbitration and appeal.

---

[35] For a survey of the practice of the UDRP see *Success by Default: A New Profile of Domain Name Trademark Disputes under ICANN's UDRP* (Syracuse University, June 2002) at http://dcc.syr.edu/markle/markle-report-final.pdf. This points to evidence that the selection of precedents in cases is skewed towards complainants, that complainants are too likely to be successful if the respondents fail to submit responses, that the elastic notion of 'bad faith' has been stretched to the benefit of complainants, and that legal emphases on the intellectual property of complainants have outweighed interests in freedom of speech. For evidence that "forum shopping" relates to the efficiency and speed of the arbitrator providers, not to the likelihood of favourable decisions, see *ICANN/UDRP Performance – An Empirical Analysis* (Networks, Electronic Commerce, and Telecommunications Institute, October 2003) at http://www.netinst.org/KesanGallo.pdf.

[36] For a comparison of the original UDRP arbitrator providers see *Fair.Com?: An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP* (Brooklyn Journal of International Law, volume 27 pages 903-938, April 2002) at http://www.brooklaw.edu/students/journals/bjil/bjil27iii_geist.pdf. This indicates that (at least until February 2002) complainants were successful in 81% of cases with WIPO and 83% of cases with NAF but only 61% of cases with eResolution; also 56% of all NAF single-arbitrator cases were decided by only six people and complainants were successful in 95% of these, and WIPO had never selected for single-arbitrator cases particular members of the roster who had published articles that could be construed as favouring respondents. Of course eResolution went out of business. There have been attempts to refute obvious inferences from this and other studies about changing the UDRP. For a list of documents including these see *Staff Manager's Issues Report on UDRP Review* (ICANN, August 2003) at http://www.icann.org/gnso/issue-reports/udrp-review-report-01aug03.htm. The UDRP is supposed to represent a consensus and would take years to change.

[37] See *Uniform Domain Name Dispute Resolution Policy* at http://www.kenic.or.ke/index.php?option=com_content&task=view&id=35&Itemid=47.

- Appointing some individuals (rather than organisations) to handle arbitration and appeal[38].
- Ensuring random assignment of arbitrators to cases, or at least limiting the numbers of cases handled by particular arbitrators.
- Providing the option of having three arbitrators instead of one, at the request of either disputant.
- Training further individuals in the country with the aid of those already appointed to handle arbitration and appeal.
- Having annual assessments of the quality of decisions by independent external advisers.

To avoid "forum shipping" disputants should not be allowed to choose organisations that can arbitrate or act as arbitrator providers. In fact organisations analogous to the UDRP arbitrator providers are not obviously useful: such organisations do not perform arbitrations, they choose arbitrators, many of whom are on the rosters of multiple arbitrator providers, so they might merely add delay and expense to a function that the ccTLD manager could do.

[38] Not many arbitrators are needed: for New Zealand, with 200,000 domain names, there are 8 and for the UK, with 4,700,000 domain names, there are 35.

7 Technical operations associated with domain names

7.1 Operating domain name servers

By contrast with the other main functions of the ccTLD manager, the function of operating the domain name servers does not raise many policy questions. ICANN requires that a ccTLD manager provide:

- A primary name server and a secondary name server with IP connectivity to the internet.
- An administrative contact in the country.
- A technical contact.
- Connectivity by email for the entire management, staff, and contacts.
- Information about the status of the domain.
- Timely responses to requests.
- Continuing access to all zones of the domain.
- Accurate, robust and resilient operation of the data base, checked by access to zones.

Avoiding security problems requires careful configuration of the ccTLD name servers. They are 'authoritative' for replying to requests about names in the ccTLD. In fact:

- They should ignore information returned by name servers that is not directly relevant to their queries. Otherwise they are especially vulnerable to security exploits, such as attempts at 'pharming'[39].
- They should not need 'recursion'. It is allowed by default in many name servers but must be disallowed in 'authoritative' name servers, as otherwise they may be implicated in amplified distributed denial of service attacks on DNS[40].
- They should restrict and authenticate zone transfers and dynamic updates that can change DNS information.
- They should avoid the security vulnerabilities found in many versions of domain name servers[41].

The operating procedures and technologies of the ccTLD manager should be as rigorous as they can in preventing fraudulent changes to DNS information, and auditing the security of the ccTLD name servers should be seen as central to auditing the implementation of ccTLD management. However, saying more than this, by describing the implementation of DNS security, is outside the scope of this report.

---

[39] A name server that replies to requests about names in other domains usually has a cache containing replies to recent requests that can be used instead of forwarding the request. The cache can be "poisoned" by putting false information in it. Normally "pharming" involves poisoning the cache of a name server to bring users to a false bank or other web site. Deploying DNS SECurity (DNSSEC) on name servers would greatly reduce the risk of poisoning but poses operational problems.

[40] For a full discussion of such attacks see *DNS Amplification Attacks* (March 2006) at http://www.isotf.org/news/DNS-Amplification-Attacks.pdf.

[41] For an account of how to do this see *Securing an Internet Name Server* (CERT, August 2002) at http://www.cert.org/archive/pdf/dns.pdf.

7.2 Publishing registration information

Among the purposes of the ccTLD manager is to manage the operation of a searchable 'whois' data base containing information on registrations within the ccTLD.

The 'whois' data base was devised to provide information about registrations so that people could be contacted when technical problems arose. The information sometimes includes contact details such as postal addresses and telephone numbers that can be used for purposes completely different from those of domain management and that may violate privacy laws.

The constituencies of ICANN debate whether this information is desirable in the 'whois' data bases for gTLD. As found by the generic Names Supporting Organisation (gNSO)[42]:

- Non-commercial users want 'whois' data to be unavailable to potential exploiters.
- Commercial users want 'whois' data to be available for checking internet uses.
- Intellectual property experts want 'whois' data to be available for checking registrants.
- ISPs want 'whois' data to be available for resolving network problems.
- Registrars want 'whois' data to be available for validating transfers of registrants between registrars but to be otherwise unavailable to competing registrars.

Part of this debate is due to potential conflicts between the requirements of ICANN and the widely accepted norms of data protection included in national data protection acts. The 'whois' data base should be formed and used in ways that comply with these norms, which conventionally include[43]:

- Specifying clearly the purposes for which information may be used.
- Limiting the information collected to what is required for these purposes.
- Permitting persons from whom information is collected to prevent it from being passed on by the intended users.

In the case of the ccTLD 'whois' data base the potential purposes of the information include:

- Resolving network problems (which requires the name server IP addresses to be available).
- Validating requests for transfers of domain names between registrars or registrants (which requires the contact details of registrars and registrants to be available).
- Identifying individuals that may need to respond to complaints about rights to names (which requires the contact details of registrants to be available).

---

[42] See *Preliminary task force report on the purpose of 'whois' and of the 'whois' contacts* (gNSO, January 2006) at http://gnso.icann.org/issues/whois-privacy/prelim-tf-rpt-18jan06.htm.

[43] For an early expression of such principles see *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Organisation for Economic Co-operation and Development, 1980) at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html. For a recent expression see *APEC Privacy Framework* (Asia-Pacific Economic Co-operation, 2005) at http://www.apec.org/apec/enewsletter/jan_vol7/onlinenewsd.primarycontentparagraph.0001.LinkURL.Download.ver5.1.9. For a short summary of the law in the UK see *Data Protection Act Factsheet* at http://www.informationcommissioner.gov.uk/cms/DocumentUploads/Data%20Protection%20Act%20Fact%20V2.pdf. There are laws having similar principles to those in the UK in Argentina, Canada, Japan, New Zealand and throughout the EU, for example.

- Identifying organisations that use domain names in email or web site addresses, for example (which requires the contact details of registrants to be available).

Not all of these details need to be available to the general public; some need to be available only to the ccTLD manager, not to registrars. However, identifying organisations from domain names is mainly intended to increase public confidence in the organisations, so it requires contact details to be available to the general public. In fact:

- If identifying organisations from domain names is an intended use of the ccTLD 'whois' data base, then registrants should be obliged to make contact details publicly available. However, access to the data base by automated processes should be prevented (by insisting on the retyping of 'hand written' images).
- If identifying organisations from domain names is not an intended use of the ccTLD 'whois' data base, then registrants could be allowed to opt out of making contact details publicly available. This would be so even for registrants using domain names in connection with their businesses.

8 The mapping of telephone numbers to domain names

8.1 The motivation for ENUM

Voice Over IP (VOIP) lets calls be set up from IP terminals to traditional phones. If IP terminals can themselves have phone numbers, VOIP lets calls be set up from IP terminals to IP terminals. However, just doing this might not provide the best possible routing of calls: it can lead to indirect routes, with a call leaving the calling party network of one IP terminal through a gateway into an intermediate traditional network, traversing that network, and entering the called party network through another gateway. The intermediate traditional network would offer more routing information; however, it would also convert between VOIP and its own representation of voice, thereby increasing call costs and decreasing call quality.

To make routes direct for calls using phone numbers, an IP network needs to find routes towards other IP networks by inspecting the phone numbers. In fact a network may find several IP communication services (such as email, fax and voice mail), with different routes, for each phone number. Some routes may use direct IP connections and other routes may pass through gateways into traditional networks.

8.2 The transformation using ENUM

The tElephone NUmber Mapping (ENUM) defines a transformation of phone numbers into domain names that can then be looked up using DNS. The transformation simply takes any phone number, removes any national prefix omitted in international dialling, completes the number with the country code, removes all characters other than digits, inserts '.' between adjoining digits, reverses the order of the digits and appends '.e164.arpa'; for instance, for South Africa (where '0' is the national prefix and '27' is the country code), the phone number 0 19 234 5678 would be transformed thus:

- Take any phone number: 0 19 234 5678.
- Remove any national prefix omitted in international dialling: 19 234 5678.
- Complete the number with the country code: +27 19 234 5678.
- Remove all characters other than digits: 27192345678.
- Insert '.' between adjoining digits: 2.7.1.9.2.3.4.5.6.7.8.
- Reverse the order of the digits: 8.7.6.5.4.3.2.9.1.7.2.
- Append '.e164.arpa': 8.7.6.5.4.3.2.9.1.7.2.e164.arpa.

Figure 5 shows how the result fits the hierarchy of domain names.

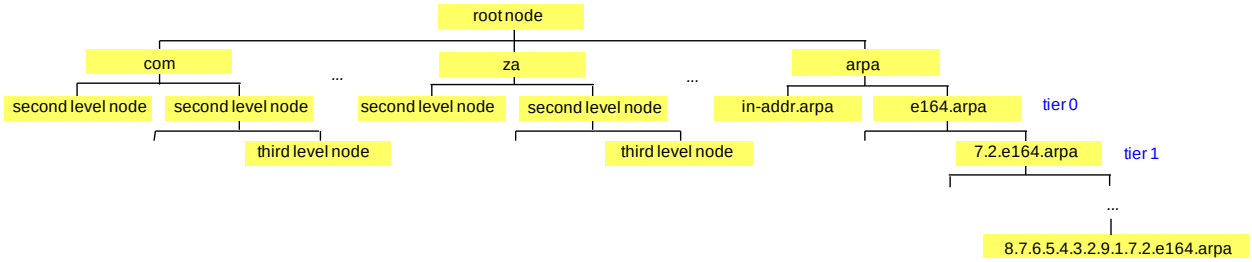

Figure 5 Structure in the '7.2.e164.arpa' domain

Looking up a domain name using DNS can provide a list of services used by the holder of the phone number, with the communication preferences of the holder; for instance, the list might indicate that the person would prefer using VOIP at person@bigglobalcompany.co.za to using email at person@ bigglobalcompany.co.za, by appearing thus:

- tel:+27-19-234-5678.
- sms:+27-70-234-5678.
- sip:person@bigglobalcompany.co.za.
- mailto:person@ bigglobalcompany.co.za.
- http://www.person.nom.za.

8.3 Systems related to ENUM

There are other systems for finding IP addresses from phone numbers. Some use DNS in the same way as ENUM but do not use the 'e164.arpa' domain. Others do not use DNS but instead have entirely different implementation techniques[44]. The most important distinction between these systems concerns whether service providers or users can supply information to, and get information from, these sources. For ENUM itself, the systems are:

- **Carrier, or infrastructure, ENUM**. Service providers supply information about the phone numbers and preferred communication services of their customers, and other service providers can get that information. The preferences in this case are likely to be those of the service providers; in fact service providers may not have, or may not wish to supply, information about all the communication services preferred by their users[45]. As carrier ENUM is used just by service providers instead of users, it can associate phone numbers with gateways between networks, not just with handsets, and can therefore be deployed for trunk networks that use IP even when the access networks do not use IP.
- **User, or public, ENUM**. Users supply information about their phone numbers and preferred communication services, and other users can get that information. The preferences in this case are those of the users and can include all of the communication services that the users take.

ENUM is supposed to adopt the domain 'e164.arpa', not the ccTLD. Formally, ENUM management in a country is not related to ccTLD management. However, ENUM introduces policy problems similar to, but more severe than, those due to the use of the 'whois' data base described in section 7.2, as discussed in Section 8.6. In fact the ENUM data base represents the more severe threat to privacy because it may include several forms of addressing and entries for all telephone subscribers, not just for domain registrants. If ENUM is to be used similar constraints on data collection and publication should apply to it as to the 'whois' data base.

[44] The term 'ENUM' should really be used only for a system that has a centralised implementation using a particular mapping of phone numbers to domain names in the e164.arpa domain.

[45] For example, if a user has a phone number and an address sip:person@one-isp.net.za provided by one service provider, that service provider may be unwilling to update the information when the user replaces the address with, say, sip:person@another-isp.net.za from a different service provider.

8.4 National organisation for ENUM

When an IP network finds other communication services from phone numbers, the phone numbers are just treated as familiar unambiguous names; other naming systems could be devised and used instead. VOIP service providers could choose to by-pass the national number allocation arrangements by adopting their own numbers looking like phone numbers. These numbers would provide VOIP but would not give access to traditional networks; they could even cause number changes when they are finally found to conflict with the national numbering plan[46].

To ensure that only valid numbers are used, there needs to be agreements between the service providers and any central authority. For ENUM this central authority is provided at the global level by ITU and at the national level by a neutral organisation working with the telecommunications regulator and the organisation operating the DNS servers. The organisation operating the DNS servers is not necessarily the ccTLD manager, because the DNS servers are those for a subdomain of 'e164.arpa', not for the ccTLD. In particular, the DNS servers for carrier ENUM might be exploited also for number portability and, as such, would be operated by the organisation responsible for a centralised number portability data base.

There needs to be one authoritative primary source of the ENUM information; secondary sources may then extract this information for consultation by service providers or users. (A similar primary source of information is needed also for directory enquiries and number portability.)

8.5 International experience of ENUM

The ENUM standard was laid down by the Internet Engineering Task Force (IETF)[47]. It deals mainly with the transformation of phone numbers into domain names, the identification of services for communication, and the format and content of DNS records. It does not deal with various related technical matters (such as DNS security, which is the subject of several other IETF documents) or organisational and political matters.

The organisational matters were taken up by the ITU, which described distinctions between the organisation responsible for managing a domain, the organisations (registries) responsible for operating the servers and the organisations (registrars) responsible for registering names on behalf of users (registrants), both globally and nationally, and discussed the security problems for users[48].

The political matters remain; they include questions over what should be the top level domain, which is currently 'arpa', controlled by ICANN and indirectly subject to the United

---

[46] Some VOIP service providers in the US may be risking doing this, by giving users numbers that are too long to conform with E.164 but that start with NPA codes not allocated in the NANP.

[47] For successive versions of this standard see *E.164 number and DNS*, RFC 2916 (IETF, September 2000) at http://www.ietf.org/rfc/rfc2916.txt, and *The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)*, RFC 3761 (IETF, April 2004) at http://www.ietf.org/rfc/rfc3761.txt.

[48] For full descriptions see *Operational and administrative issues associated with national implementations of the ENUM functions*, ITU-T Recommendation E.164 Supplement 3 (ITU, May 2004) at http://www.itu.int/rec/T-REC-E.164-200405-I!Sup3, and *Operational and administrative issues associated with the implementation of ENUM for non-geographic country codes*, ITU-T Recommendation E.164 Supplement 4 (ITU, May 2004) at http://www.itu.int/rec/T-REC-E.164-200405-I!Sup4.

States (US) Department of Commerce, and what should be the ENUM registry at a global level, which is currently RIPE-NCC, with its main function being to allocate IP addresses in Europe. These questions are now before the Internet Governance Forum created by the World Summit on the Information Society (WSIS). In the interim, some service providers are introducing systems that work like ENUM but are "unofficial" and not encumbered by such questions.

Despite these problems, there have been trials of ENUM in several countries. Often these have been led by enthusiasts for ENUM, but sponsored by the governments. Following these trials the governments are now considering whether the benefits of deployment justify active support. There are now various plans for deploying ENUM, either as carrier ENUM (in Poland and Romania) or as user ENUM (in Austria, the Czech Republic, Germany and Ireland)[49].

However, so far ENUM has not been adopted rapidly. In particular, user ENUM suffers because the commercial drivers for it are weak. However, carrier ENUM has fewer disadvantages than user ENU, so it is favoured in principle[50].

For reasons outlined in Section 8.6, customers may well not be enthusiastic about ENUM. In some countries certain non-geographic numbers have been reserved for ENUM subscribers. Though doing this may reduce number portability implementation problems for those numbers, it could well decrease enthusiasm for ENUM further, as customers often prefer geographic numbers.

8.6 The effectiveness of ENUM

The arguments for having ENUM include:

- It lets service providers have direct routes for VOIP calls using phone numbers. It therefore helps with the growth of competition between VOIP and traditional telephony.
- It can be used by communication services other than VOIP. For example, MMS was intended to use ENUM (though in fact it is generally implemented without ENUM, partly to avoid any regulatory problems when ENUM information is shared internationally between service providers).
- It can be used in implementations of traditional network features like number portability and specially tariffed numbers, because it has a centralised implementation.
- In the form of user ENUM, it could provide something having similar effects to portability of domain names (for email addresses, for example); users would tell people their phone numbers, not the addresses of their communication services[51].
- In the form of user ENUM, it could let users make personal information available globally for new internet applications just by using phone numbers as a naming system.

---

[49] For a report on the status of ENUM in many countries, maintained by Réseaux IP Européens (RIPE), which provides co-ordination support for ENUM delegations, see http://enumdata.org. The report may not be not fully up to date; that in itself could indicate something about the general level of enthusiasm for ENUM.

[50] There may be plans for deploying carrier ENUM that are not widely known, because unlike user ENUM it does not need to use the e164.arpa domain and does not need to be recorded with RIPE.

[51] For example, a user having phone number +27 19 234 5678 might switch from using sip:person@one-isp.net.za to using sip:person@another-isp.net.za without telling other users: 8.7.6.5.4.3.2.9.1.7.2.e164.arpa would act as a domain name for the user.

The trials mentioned in Section 8.5 have shown that user ENUM presents various problems that carrier ENUM does not present. The main problems are:

- User ENUM lets people read user information about others. It thereby makes "spamming" (communicating with someone else without any implied consent, particularly through email) and "spoofing" (pretending to be someone else) easier. This sort of abuse could be limited by restricting user ENUM to users who opt in; there could even be a special number range, from which users would be get numbers only if they opted in to user ENUM. However, restricting user ENUM to users who opt in merely limits this sort of abuse, without eliminating it, and reduces the potential market for user ENUM[52].
- User ENUM lets people try to change user information about others. The changes could be intended for "slamming" (transferring the service for a user to another service provider without consent) or for redirection, perhaps to steal traffic containing business information. Consequently users need to be authenticated before they change their information. Often the service provider to whom a number has been allocated and with whom the user has a billing relationship could do this authentication readily. However, the service provider might not help, believing that user ENUM wastes effort or even reduces revenue (by replacing phone calls by email, for example). Extra ways of authenticating users are needed, just as they are for carrier selection and number portability.
- Users who opt in to user ENUM are likely to keep their user information correct only until they stop using the numbers. Moreover, service providers may not check that the information is correct, especially when it applies to their former customers. If the system includes incorrect information then new "owners" of these numbers may be denied access or may have communications misdirected.

Though user ENUM gives a new role to phone numbers (and to DNS, in a centralised implementation), the value of this is debatable, for the following reasons:

- To use user ENUM, callers need to know phone numbers first. Directories indexed by the names of contacts are more generally useful, especially as they identify the communication services for an individual contact, not for all the people with which that contact shares the phone number.
- By using user ENUM, callers may be able to find email addresses (for example) from phone numbers but they will not be able to find phone numbers from email addresses. Other services would be needed to supply such information.
- Though user ENUM resembles a "find me / follow me" service (which lets calls track the locations and availability of users), it is not one, because DNS deliberately does not support rapid updating by users. Consequently any users wanting a "find me / follow me" service would need to get it separately and might not then bother to maintain their records in user ENUM.
- Though user ENUM adopts phone numbers as a naming system, the names are not usually unique to particular individuals, at least for fixed access networks (in which all the members of a household share one number). Mobile numbers tend to be personal, but VOIP is currently associated more with fixed access networks than with mobile access networks. Personal numbers, when distinguishable from mobile numbers and nomadic numbers, have not been very successful so far. Consequently user ENUM is not always appropriate to holding personal preferences about communication services.

[52] Users could also reduce the loss of privacy by imposing SIP called party control and providing only addresses containing SIP aliases, not their usual names, to DNS.

Abbreviations

AfriNIC	African Network Information Centre
AfrISPA	African Internet Service Providers' associations' Association
AfNOG	African Network Operators' Group
AfTLD	African Top Level Domains
APEC	Asia-Pacific Economic Co-operation
ccNSO	country code Names Supporting Organisation
ccTLD	country code Top Level Domain
CENTR	Council of European National Top-level domain registries
CERT	Computer Emergency Response Team
DNS	Domain Name System
ENUM	tElephone NUmber Mapping
EU	European Union
GAC	Government Advisory Committee
gNSO	generic Names Supporting Organisation
gTLD	generic Top Level Domain
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IP	Internetwork Protocol
IPv4	IP version 4
IPv6	IP version 6
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU	International Telecommunication Union
ITU-D	ITU – Telecommunication Development Sector
ITU-T	ITU – Telecommunication Standardisation Sector
LIR	Local Internet Registry
MMS	Multimedia Messaging Service
NAF	National Arbitration Forum
NCC	Network Control Centre
OECD	Organisation for Economic Co-operation and Development
RIPE	Réseaux IP Européens
RIR	Regional Internet Registry
SMS	Short Messaging Service
UDRP	Uniform domain name Dispute Resolution Policy
UK	United Kingdom
VOIP	Voice Over IP
WIPO	World Intellectual Property Organization
WSIS	World Summit on the Information Society