Policy, Business, Technical and Operational Considerations for the Management of a country code Top Level Domain (ccTLD)

APRIL 2008 DRAFT

For further information, please contact the
ITU-D ICT Applications and Cybersecurity Division at
<cybmail@itu.int>

draft

International Telecommunication Union

Acknowledgements

The objective of this report is to outline the numerous technical and procedural aspects of establishing and operating a ccTLD (Country Code Top-Level Domain) registry.

This draft report was commissioned by the ITU Development Sector’s ICT Applications and Cybersecurity Division and prepared by Mr. Jim Reid, RTFM Ltd., Bothwell, Scotland.

Many thanks to Robert Shaw, Head of the ICT Applications and Cybersecurity Division, for initiating this project. Several people, including Jaap Akkerhuis, Rob Austein, Ayitey Bulley, Brian Candler, John Klensin, Andy Linton, Dave Meyer, Mike O'Dell, and Oscar A. Robles-Garay have made suggestions or offered editorial comments about earlier versions of this document. These comments contributed significantly to whatever clarity the document has, but the author bears responsibility for the content.

This material is partially based upon work supported by the National Science Foundation under Grant No. NCR-9981821. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

For further information and to make comments on this document, please contact:

ICT Applications and Cybersecurity Division (CYB)
Policies and Strategies Department
Bureau for Telecommunication Development
International Telecommunication Union
Place des Nations
1211 Geneva 20, Switzerland
Telephone: +41 22 730 5825/6052
Fax: +41 22 730 5484
E-mail: cybmail@itu.int
Website: www.itu.int/ITU-D/cyb/

Disclaimer
The opinions expressed in this report are those of the author(s) and do not necessarily represent the views of the International Telecommunication Union (ITU) or its membership. The designations employed and the presentation of material, including maps, do not imply the expression of any opinion whatsoever on the part of ITU concerning the legal status of any country, territory, city or area, or concerning the delimitations of its frontiers or boundaries. The mention of specific companies or of certain products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned.

Abbreviations

ADR	Alternate Dispute Resolution
AFRINIC	African Regional Internet Registry
AFTLD	African Top-Level Domain Organisation
BIND	Berkeley Internet Name Domain (Common DNS implementation)
ccTLD	Country Code Top-Level Domain
CENTR	Council for European National Top-Level Domain Registries
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions (Secure DNS)
EPP	Extensible Provisioning Protocol
ETSI	European Telecommunications Standards Institute
gTLD	Generic Top-Level Domain
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IDN	Internationalised Domain Name
IETF	Internet Engineering Task Force
IGF	Inter Governmental Forum
ISOC	Internet Society
ITT	Invitation To Tender
ITU	International Telecommunication Union
RFC	Request For Comments (Internet Protocol Specification Document)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
UDRP	Uniform Dispute Resolution Policy
URL	Universal Resource Locator (web address)
WIPO	World Intellectual Property Organisation

Table of Contents

1 Executive Summary

The objective of this report is to explain the numerous technical and procedural aspects of establishing a ccTLD (Country Code Top-Level Domain) registry. It describes the processes involved in the reassignment of administrative control of a ccTLD and the associated issues and anticipated time-lines in achieving this goal.

Readers of this report are also recommended to review the related materials in the *ITU Handbook on Internet Protocol (IP)-Based Networks and Related Topics and Issues* (2005) available in Arabic, Chinese, English, French, Russian and Spanish on the ITU Development Sector's ICT Applications and Cybersecurity website[1]. In particular, Chapter 4.3.2 in this Handbook refers to country code Top Level Domains (ccTLDs).

This report considers a number of factors related to ccTLD management that need to be considered. These include the potential governance models and structures to be used for the ccTLD, drawing from examples of best practice that are used in the Internet today and discusses the advantages and disadvantages of these models. An analysis of how ccTLDs structure their name spaces is presented, explaining how particular approaches affect aspects of the registry's operations and policies.

A discussion of typical governance models and registry structures is presented. Extensive information is given on the registry policy considerations that are necessary for deciding how the registry operates. It gives advice on the technical aspects of running a registry: systems, interfaces, processes, support and service levels. Guidance is also provided on how a ccTLD could be relaunched. The report suggests how registry personnel could engage with Internet fora and meetings that are involved in registry policy formation, standards formation and liaison with peer organisations.

The report also describes a wide range of policies that are needed for routine operations of a registry. These include eligibility criteria (i.e., who is allowed to register names in which parts of the name space), pricing considerations, contracts, escrow arrangements, registry-registrar agreements and dispute resolution. Advice is also given on how to formulate registry policy and how the Administration could be involved in these deliberations. Many of these are matters of routine registry operations and may not need much regulatory or government oversight.

Technical considerations are also explained in some detail. These include information about the software and systems needed to provide a stable ccTLD registry. The report outlines the various components of a registry's infrastructure: databases, DNS name servers and whois servers, operational practices and access controls. Performance metrics, service level agreements and technical interfaces are discussed. Some guidance on the likely skills and expertise for registry staff is also provided. Training and mentoring of the registry's staff will be needed and the report suggests how these can be provided. A discussion of emerging technologies and technology trends that should be part of the future plans for the registry is also presented.

The report summarises the typical outreach activities that a registry should carry out. These would include engagement with the government and the general public. Interaction in a number of international fora such as ICANN and IETF that are involved in policy-making and protocol development is recommended. Those who are responsible for the ccTLD registry are also advised to participate in membership organisations like AFTLD or CENTR who organise workshops and meetings where registry management and technical staff discuss common approaches and devise best practices in registry operations. These will provide opportunities for the ccTLD registry to engage with its peers as well as the wider Internet community.

As a generic document, this report cannot consider in detail an Administration's public policy goals for its ccTLD or Internet usage. Even so the report underlines that the ccTLD registry should be set up and operated according to those goals. These public policy objectives should provide the foundations for the registry and its governance structure.

[1] http://www.itu.int/ITU-D/cyb/ip/

Assuming control over a ccTLD consists of essentially two tasks. The first of these is gaining administrative control of the ccTLD by becoming the Sponsoring Organisation in the IANA database. This responsibility can rest with a government department or regulatory authority or it can be outsourced to various degrees. The Administration will generally set terms or reference or provide some kind of legislative instrument to define the powers and scope of responsibility for the Sponsoring Organisation. The second task is for the Sponsoring Organisation which has to develop and implement a governance structure and policy making framework for the ccTLD registry, usually through contracts or other agreements. In simple terms, the Administration decides who the Sponsoring Organisation should be for its ccTLD. The Sponsoring Organisation then decides who should operate the registry for the ccTLD and how it is to be governed. If the registry operator fails to meet its obligations or a new model is needed, the Sponsoring Organisation should be able to select a new registry operator. Likewise if the Sponsoring Organisation fails to meet its obligations or a new legislative framework is introduced, the Administration can decide to transfer that responsibility.

Finally, the report suggests an outline plan that could be used by to develop a ccTLD registry from its current state to one that fully engages with the local Internet community and addresses an Administration's public policy objectives for Internet usage. These include administrative, policy, technical and business considerations. It is likely that this development process will take some time, perhaps a year or more. Production and execution of a business plan for the registry would be a very important component of this activity. This section of the report assumes that the Administration has made substantial changes to the ccTLD, for example by changing the registry operator or as a result of a radical overhaul of the registry's policies. These far-reaching changes would presumably be the consequence of a review of the Administration's public policy goals.

It is intended that the audience for this report has some familiarity with the functions and roles of the organisations involved in Internet matters and the relationships between them. This report has tried to keep the use of technical jargon to a minimum. Even so, some use of Internet terminology is unavoidable in a report of this nature. As far as practically possible explanations are provided whenever technical terms are introduced.

2 INTRODUCTION

In simple terms, the DNS translates domain names such as www.itu.int into IP addresses. A registry maintains a list of domain names that have been registered and arranges for these names to be published in the DNS. For resiliency and robustness, each zone (logical administrative unit) in the DNS is served by more than one name server and these are distributed in different locations to avoid single points of failure. Updates to the zone are performed on exactly one server known as the master name server and propagated from there to the other servers which are known as slaves. The DNS protocol automatically takes care of synchronisation and replication of data between the master name server and the slave name servers for each zone. Master servers were known as primary servers and slaves used to be called secondary servers. These terms are identical and are sometimes used interchangeably. Master and slave are the terms used in current DNS jargon.

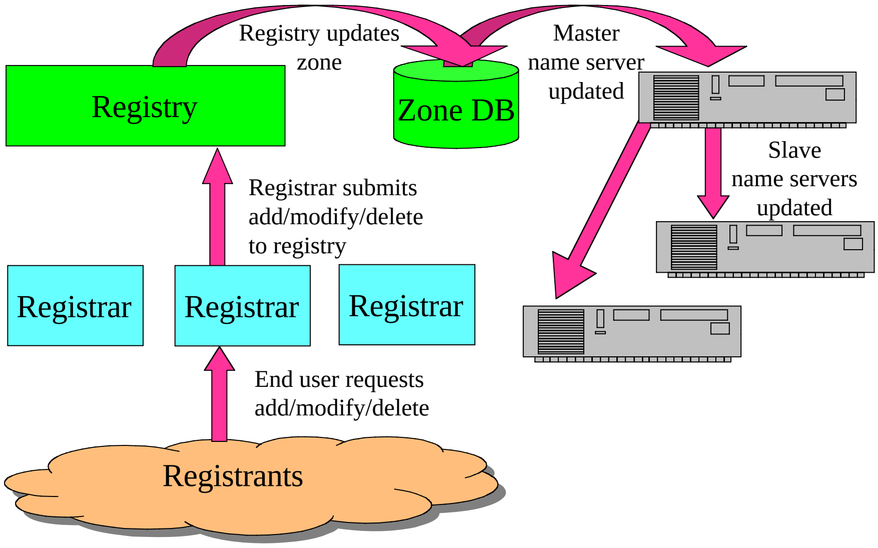

Registry updates zone
Master name server updated
Registry
Zone DB
Slave name servers updated
Registrar submits add/modify/delete to registry
Registrar
Registrar
Registrar
End user requests add/modify/delete
Registrants

Figure 1 — Roles and Data Flows in a Conventional Registry

Figure 1 illustrates the general model that is used in the domain name business. End users are the organisations or individuals who hold and register domain names. These are known as *registrants*. A registrant will generally have a business relationship with a *registrar* to register domain names on their behalf. Registrars are typically Internet Service Providers (ISPs) or companies that offer other services such as web and mail hosting. Registrars interact with the *registry* which maintains a database of registered domain names. This database is used to populate the registry's Domain Name System (DNS) and whois servers.

Registries are by definition a monopoly. There can only be one registry for a DNS zone and each DNS zone is unique. Therefore there can only be one registry for any ccTLD or gTLD. There is only one `.int` TLD for instance, so there is exactly one registry which maintains and publishes the list of `.int` domain names. Since the registry is a monopoly function, there may be restrictions on its business and mode of operations because of prevailing competition law. A small number of companies offer generic registry services, providing economies of scale by sharing infrastructure between TLDs. There are usually many registrars for a TLD, competing on a number of grounds: price, service, customer support, value-added features and so on.

A registrant can be considered to be the "owner" of a domain name. For all practical purposes, they do own the name even though the concept of domain name ownership is not well defined in property law. Domain names are registered for a number of years depending on the registry's rules and the fees that are paid. At the end of a domain name’s registration period the registrant can renew the registration. If they let the registration lapse, the domain name may become available for someone else to register. Sometimes domain names are transferred between registrants. Although the terms “domain name holder” and “domain name owner” are used interchangeably, it is more strictly correct to use the former.

It should be appreciated that there is an even wider group of end users: the people and organisations who use the Internet. They will depend on the data returned from the DNS so that they can visit the web sites, send email and use other forms of Internet-based communication to contact those who have registered domain names. There is a responsibility to this wider set of users — the Internet community as a whole — even though they are unlikely to have any sort of business relationship or agreement with any of the parties shown in Figure 1.

The whois service is independent of the DNS. It provides information on the status of domain names: technical, administrative and billing contact details about the domain name holder; which registrar was used; when the domain name was registered; when it was last updated; the domain’s expiry date; and so on. The information displayed by each registry’s whois server varies. It can depend on factors such as the prevailing national law (particularly those on Data Protection and privacy), contractual obligations and registrant or registrar preferences.

It should be noted that the report makes a distinction between the *registry* and *registry operator* which may not always be explicit. In places, the difference is obvious from the context. In others it is implied. As a general guide the term “*registry*” or “*ccTLD registry*” refers to the entity that oversees the operation of the systems and policies for the ccTLD. This may or may not be the same as the “*registry operator*”: the entity that provides the underlying infrastructure of systems and procedures for registering domain names. These may well be the same organisation but do not necessarily have to be. For instance the *ccTLD registry* could have responsibility for managing a policy-making framework and arranging a contract with a *registry operator* for the provision of registry services.

3 Obtaining Control of a ccTLD

It is clearly a matter of concern for many Administrations that they take control of their ccTLD, the country-code top-level domain which usually is a matter of national sovereignty.

IANA, the Internet Assigned Numbers Authority, maintains the data for the Internet root zone and co-ordinate any changes to it. These responsibilities include the delegation of new top-level domains (TLDs) and updates to existing TLDs. All changes to the Internet root zone entail IANA liaising with the US Government's Department of Commerce and Verisign, the US company that operates the master name server for the root zone. IANA is part of ICANN (Internet Corporation for Assigned Names and Numbers), the US not-for-profit corporation responsible for global co-ordination of the Internet.

An Administration can obtain control over its ccTLD by registering an appropriate entity as the Sponsoring Organisation in the IANA database. In earlier days of the Internet, the Sponsoring Organisation would usually have been the entity which originally obtained the delegation for a ccTLD, typically a Computer Science department at a university. Although these informal arrangements would have been acceptable at that time, they are generally unsatisfactory for the current environment where stewardship of national Internet resources is an important matter that has many public policy implications.

Sponsoring Organisations and operators of TLDs do not have contracts or agreements with IANA. Some have contracts with ICANN, IANA's parent body. A number of ccTLDs have entered into agreements with ICANN. A few types of agreement are possible and the one used for a ccTLD depends on which is most comfortable for the Administration or Sponsoring Organisation. Some have executed a standard ICANN framework agreement. Others have used an exchange of letters or a Memorandum of Understanding (MoU). No matter which type of agreement is chosen, it tends to be described in a lightweight document which essentially just offers mutual recognition of each party's responsibilities.

Copies of these agreements and details of which countries which have executed them can be found on the ICANN web site at http://www.icann.org/cctlds/agreements.html. It is advisable for an Administration to enter into some sort of agreement with ICANN. However this is not mandatory. ICANN and IANA do not insist that a change of Sponsoring Organisation is tied to completion of a mutual recognition agreement or that an existing agreement prevents future changes to a ccTLD's Sponsoring Organisation.

Since IANA has no formal procedure for a change of Sponsoring Organisation, the process IANA follows is somewhat *ad-hoc*. The general idea that underpins a change of Sponsoring Organisation is support from the local Internet community. This is a rather nebulous concept. It is not necessarily the case that a request from a government or regulator will be accepted at face value by IANA. In some parts of the world, government authorities and the local Internet community do not agree who the Sponsoring Organisation should be! IANA tends to wait until consensus emerges before acting in such cases.

3.1 Overview of Redelegation Process

In principle it is a straightforward task to change the Sponsoring Organisation for a ccTLD in the IANA database. This is a procedure which IANA carries out several times a year, usually at the request of the government or regulator for the country concerned. There will normally be no documented agreement between IANA/ICANN and the entity requesting the change of Sponsoring Organisation. In fact it is usually some sort of failure of the current Sponsoring Organisation that triggers the redelegation request. In this context, it should be noted that "redelegation" means change of Sponsoring Organisation. It does not mean redelegation in the strictly technical use of that term in DNS: i.e. changing the name servers for some zone. Changing the Sponsoring Organisation does not necessarily imply or require changes to the DNS infrastructure for the TLD.

It is best that any changes of a technical or administrative nature to a TLD are not combined. If an Administration plans to change its ccTLD's Sponsoring Organisation and change the name servers for the ccTLD, these should be done separately. The best approach will be to first complete the change of Sponsoring Organisation. The new Sponsoring Organisation can then co-ordinate the technical DNS changes needed for alterations to the ccTLD's name servers.

The procedure for transferring the ccTLD to the Administration is fairly simple and should not be unduly time-consuming. In outline, an authorised representative of the Administration can write to IANA requesting that the ccTLD be redelegated. This will initiate the process described below. Full details are given in Annex A.

On receiving the redelegation request IANA will try to contact all interested stakeholders to verify the information and to ensure that they agree with the proposed redelegation. Normally it is sufficient that the current and new Sponsoring Organisations confirm in writing to IANA that they agree to the change. Agreement by the current registry operator and Sponsoring Organisation — assuming they are not already parties to the change request — is also helpful. Where possible, IANA will also consult the local chapter of the Internet Society, ISOC. When there is no active ISOC chapter in a country IANA will look for wider expressions of support for changing the Sponsoring Organisation for the ccTLD. These should come from the local Internet community such as representatives of appropriate trade associations, academia, user groups and so on. Ideally, there should be a broad range of support from other institutions such as Chambers of Commerce, trade unions, local authorities, consumer groups and non-governmental organisations.

Once IANA's requirements have been satisfied, a recommendation will be made to the ICANN board, which will normally vote on this at their next meeting. ICANN Board meetings are generally held on the 15th of each month. After the ICANN Board approves IANA's recommendation, IANA then submits a report to the US Government's Department of Commerce for further administrative checks. These checks are usually completed within one business week. The Department of Commerce then co-ordinate with IANA and Verisign, the technical maintainer of the Internet root zone database, to update the Internet root zone. This results in the new ccTLD delegation information being published by all the Internet root name servers and thus being made visible to the global Internet community.

Under normal circumstances, this process tends to take 6-8 weeks of elapsed time. However there are some special circumstances that may complicate matters. These are described below.

3.2 US OFAC Regulations

The redelegation process involves IANA, which is part of ICANN, an organisation incorporated in the United States of America. It will also entail interaction with the US Department of Commerce (DoC). Both are bound by US law. The US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals. These are applied through the Office of Foreign Assets Control, OFAC. There are severe penalties for US citizens and organisations who violate OFAC regulations.

OFAC maintain a Specially Designated Nationals (SDN) List. This list is available on the Internet at: http://www.treas.gov/offices/enforcement/ofac/sdn/index.shtml. US citizens and organisations are generally prohibited from dealing with entities on the SDN List. It is recommended that any redelegation request from an Administration is not associated with any of the individuals or organisations on the SDN list. If this is not possible, ICANN and the Department of Commerce can apply for an exemption from the OFAC regulations so that they can satisfy an Administration's redelegation request. However this application would take time and is likely to generate further bureaucratic and administrative obstacles.

3.3 Changing ccTLD Name Servers

Changes to the ccTLD's name servers require completion of a template containing technical details of the new name servers. This template can be submitted by the administrative or technical contacts for the ccTLD registry. Usually there is no need for government involvement in these changes which are of a technical and operational nature. These changes rarely have any public policy considerations. A sample template is shown in Annex A.

IANA will verify the information provided in the template. IANA will also need to know the names and IP addresses of the DNS servers for the ccTLD. This is critical to the technical task of changing the delegation information in the Internet root zone. To ensure the stability and security of the Internet, IANA will also check that the new DNS servers are functioning correctly before the redelegation is performed.

Updates to a TLD’s name servers and DNS delegations are normally processed in less than five working days. The technical work is simple and takes very little time. However these changes entail modification of the Internet root zone file and that requires administrative approval by the US Department of Commerce (DoC). All changes to the Internet root zone entail IANA liaising with the US Government’s Department of Commerce and Verisign, the US company that operates the master name server for the root zone.

3.4 Selecting the Sponsoring Organisation

Before an Administration submits a redelegation request, it should have made a decision about which organisation should be responsible for the ccTLD. In theory this is a national matter: how a country organises the infrastructure for its ccTLD is largely an internal decision. Even so it is advisable to get broad consensus support about the choice of Sponsoring Organisation. It is unlikely that a change of Sponsoring Organisation will be processed by IANA if there is little support from the ccTLD’s stakeholders, the local Internet community. In addition it is likely that a Sponsoring Organisation will be unsuccessful if it does not enjoy local support. Consultations and discussions about registry policies will be difficult if the local Internet community does not feel its views are represented fairly or listened to.

There are several potential choices for a ccTLD’s Sponsoring Organisation. It could be part of a government department. It could rest with a regulator which may or may not be part of government. Some sort of independent entity could be the Sponsoring Organisation: perhaps a non-profit membership organisation that involves the local Internet community. Another option is to have a neutral, independent organisation that operates at arms-length from the government such as a university or a charitable foundation.

A further consideration is the extent of government control that is necessary or desirable. This will also depend on the level of responsibility that the Sponsoring Organisation should have.

The usual model is for the Administration to select a government department as the Sponsoring Organisation. This ensures the Administration can easily change the Sponsoring Organisation whenever this is needed, for instance because of new legislation or a change or government policy. The Administration could then choose to delegate responsibilities to the Sponsoring Organisation: establishing a governance model for the ccTLD registry, overseeing registry policies, executing contracts and so on. This approach can give the Sponsoring Organisation a framework to operate from that takes account of public policy objectives but at the same time leave the Administration with overall control of the ccTLD without the need to be directly involved in routine operation of the ccTLD registry.

3.5 Selecting the Registry

Changing the Sponsoring Organisation does not necessarily mean that there has to be a change of ccTLD registry. Usually a the introduction of a new Sponsoring Organisation has no operational impact on the ccTLD registry: it continues processing registration requests as before. All that essentially changes is the relationship between the registry and its Sponsoring Organisation. However if the registry is unable or unwilling to adapt to those circumstances, it may be necessary for the new Sponsoring Organisation to take action. Sometimes the change of Sponsoring Organisation will have been initiated by the Administration to achieve a change of ccTLD registry.

Changing the ccTLD registry is an extreme step. It should only be carried out as a last resort because this is a complex and error-prone operation that can be disruptive and difficult. All the data and registrations from the existing registry would probably need to be transferred to the new registry. The new registry would need to have deployed equipment and staff to take over the existing operations. Extensive testing would be needed. Considerable outreach efforts may be necessary to educate the local Internet community about the change of registry operator. There would also have to be very close co-operation between the two registries, which may be awkward. Clearly, a great deal of care and planning would be needed before taking such drastic action.

Sometimes such a change can be trouble-free. For example, the existing registry might just be spun out from its previous home at a university and set up as an independent organisation. All the staff, equipment and resources could just be transferred to the new entity. Even in these situations where the migration is amicable, the transition can be technically challenging.

3.6 Roles and Responsibilities

In essence a ccTLD has three distinct roles which may or may not be combined. It is usually a good idea to keep these roles separated since they have distinct responsibilities. However this is not always necessary. Local circumstances may suggest that some or all of these roles can be occupied by a single entity.

The Sponsoring Organisation is the entity that IANA considers is responsible for the ccTLD. It may or may not have an agreement with ICANN, IANA’s parent body. Usually the Sponsoring Organisation is a government department or regulator which oversees Internet matters nationally and is charged with implementing the Administration’s public policy goals for the Internet. The Sponsoring Organisation will generally be responsible for oversight of the governance structure and policy development processes for the ccTLD registry. It will also select the ccTLD registry. An Administration would probably only need to change the Sponsoring Organisation for its ccTLD as a result of new legislation or reorganisation of the government. It may also intervene when the Sponsoring Organisation is unable to satisfy public policy objectives.

The ccTLD registry will be responsible for the routine operation of the registry and the selection of the registry operator. The scope of this responsibility may be defined by some form of agreement with the Sponsoring Organisation. The ccTLD registry would establish and operate a governance structure that is in line with this agreement. This is likely to include stakeholder representation, development of registry policy and the technical and operational criteria for the registry itself. The ccTLD registry may enter into a contract with another organisation for the provision of registry services. This contract would document the technical and operational implementation of the actual registry. The Sponsoring Organisation would normally have the ability to replace or reorganise the ccTLD registry: for instance if the current structure is not fulfilling its obligations to the local Internet community.

The registry operator will be responsible for the registry database and the supporting infrastructure of DNS servers, whois systems and so on. It will implement the policies and processes defined by the ccTLD registry. This may be defined by a formal contract: for example if registry services are outsourced. The ccTLD registry would have the authority to introduce changes of registry policy and have them implemented by the registry operator. Ideally this would be done by a process of consensus and mutual agreement.

4 General Policy Considerations

Introduction

The following introduction is derived from Chapter 4.3.2 of the *ITU Handbook on Internet Protocol (IP)-Based Networks and Related Topics and Issues* (2005) available in Arabic, Chinese, English, French, Russian and Spanish on the ITU Development Sector's ICT Applications and Cybersecurity website[2].

A country code top level domain name (ccTLD) is a TLD used in the Internet DNS to identify a country, for example ".ch" for Switzerland. The two letters chosen for each country are derived from the ISO 3166 standard. Currently there are 243 ccTLDs. The rules and policies for registering domain names in the ccTLDs vary significantly by country. In some cases, domain names come under the provisions of a general telecommunications law and the government exercises its formal powers, or its informal influence, through the ministry of telecommunications or the telecommunications regulator, or other government ministries or agencies. The appropriate government authority may supervise the activities of the ccTLD operator and approve their pricing policy if there is not a competitive registry-registrar model.

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

In other cases, the government maintains a hands-off approach to ccTLD operations, which are left to the private or academic sector, to either not-for-profit or for-profit entities.

Some ccTLDs are reserved for use by citizens or entities of the concerned country or territory, while others are operated in an open and completely unrestricted manner.

Generally speaking, the ccTLD managers (called registries) are entities that are legally (and often operationally) resident in the concerned country or territory. In the early days of the Internet, the registries were often academic or research institutions. Today they are more often commercial or special-purpose non-profit organizations, or government-owned or licensed entities. Governments have become involved in accordance with local legal frameworks and traditions. Government involvement ranges from formal (via laws and regulations) through informal.

A key question facing national policy-makers is how best to ensure that identified public-policy goals are met by a ccTLD manager given the various models of ccTLD management used. As noted above, in some countries, the ccTLD operator is entirely free from government supervision. In other countries, there is informal influence from the government, while in yet other countries there is a formal link between the government and the ccTLD operator. Such a formal link can take several different forms: contract between the government and the operator, legislation defining the roles and responsibilities of the operator, or regulations.

For additional background information on ccTLDs, see:

- IETF RFC 1591 "Domain Name System Structure and Delegation" at http://www.ietf.org/rfc/rfc1591.txt?number=1591, which provides the basic principles and rules that have been used to implement the Internet Domain Name System and to delegate to ccTLD operators
- The ICANN webpages containing "ccTLD Resource Materials" at http://www.icann.org/cctlds/
- In February 2002, ICANN's Governmental Advisory Committee (GAC) published "Principles for Delegation and Administration of ccTLDs" at http://www.icann.org/committees/gac/gac-cctldprinciples-23feb00.htm

[2] http://www.itu.int/ITU-D/cyb/ip/

- Further information on ccTLD can be accessed through regional ccTLD organizations: APTLD for Asia Pacific (http://www.aptld.org), AFTLD for Africa (http://www.aftld.org), CENTR for Europe (http://www.centr.org), NATLD for North America, LACTLD for Latin America and the Caribbean (http://www.lactld.org)

- The list of current ccTLD contact information for each country code can be found at http://www.iana.org/cctld/cctld-whois.htm

- Information on national practices for certain countries can be found at: http://www.itu.int/ITU-T/special-projects/ip-policy/final/Attach10.doc (Attachment 10)

- Websites of particular ccTLDs accessed from http://www.iana.org/cctld/cctld-whois.htm

- ITU-T Workshop on Member States' experiences with ccTLDs, at http://www.itu.int/ITU-T/worksem/cctld/index.html

- TSB Circular 160, Addendum 2, which summarizes responses to a questionnaire on Member States' experiences with ccTLDs

- The best practices developed by a forum of ccTLD operators can be found at: http://www.itu.int/ITU-T/special-projects/ip-policy/final/Attach11.doc

- One particular generic ccTLD model can be found at: http://www.itu.int/ITU-T/special-projects/ip-policy/final/Attach12.doc

While it is obviously important for a government to have sovereignty over its ccTLD, this should be placed in the overall context of the Administration’s wider public policy goals as well as its ambitions for Internet usage. Likely objectives here may include addressing the “digital divide”; promoting Internet usage and computer literacy; nurturing and extending indigenous Internet expertise; improving the quality and diversity of the country’s Internet infrastructure; and interaction with the wider Internet community through participation in technical and policy fora such as ICANN, WSIS activities, IGF, IETF, Regional Internet Registries (RIRs) (e.g., AFRINIC) and regional top level domain associations. It may also be advantageous to engage with groups that represent diasporas or other overseas cultural and social institutions. The objective of these broad policy goals is clearly a national matter and out of scope for this document. What have been presented here are suggestions which may help inform policy making deliberations. Once these policy decisions have been made, the Administration should consider the strategies and tactics for the ccTLD which are most likely to achieve these objectives.

The tactical and strategic directions cover four broad areas. First is the nature of the registry and its governance model. Second is how the name space under the ccTLD is organised. The third area concerns the business model for the registry. The final tactical and strategic area addresses how the registry itself is operated and the technical criteria needed for running it. These are discussed in more detail below.

Annex B, References on Best Practice Guidelines for ccTLD registries, provides a summary of the broad principles of registry operations and governance that may be generally applied. It would be advisable to take account of these guidelines as when developing a framework for the national ccTLD registry.

4.1 Governance structure

There are a number of possible governance models for a ccTLD registry, each with its own set of advantages and disadvantages. Before these are considered, the regulatory and legal framework that will apply has to be taken into account. For instance, if the registry is to be a part of government or is highly regulated, certain governance models will be impractical and others would be more appropriate. Wider government policy considerations also need to be examined. These could include factors such as safeguards for consumer protection and public confidence; representative stakeholder involvement; fairness and transparency; competition issues; privacy concerns; and the broad national interest.

As a general rule, the preferred governance model for ccTLD registries is to have some independent entity which oversees the operation of the registry. These entities are often not-for-profit mutual associations or foundations, with membership open to anyone with an interest in the country’s domain name business. The

Swedish and Dutch ccTLDs operate as charitable foundations while the UK and Irish ccTLD registries exist as not-for-profit companies limited by guarantee.

Operating on a non-profit basis keeps costs down and helps to ensure the registry operates in the widest public interest. If the entity has no shareholders, it is less likely to be taken over by vested interests who have the resources to acquire control of the organisation. The absence of shareholders also means the registry is not under pressure to generate dividends and can take a broader view of its responsibilities to the public. Since the registry is essentially managed by its stakeholders, it should be responsive to their needs.

There are essentially five governance models to choose from.

4.1.1 Part of Government

From a perspective of government control, operating the ccTLD registry as a part of government is perhaps the most attractive. The registry becomes just another department of the Ministry of Posts and Telecommunications (for instance) and does whatever the government decides.

Although some registries operate as part of government, this has tended to arise for historical reasons and the general trend is to move registries away from the public sector. It could also be necessary for legislation to be passed so that a government department or a regulator had the authority to run a ccTLD registry.

4.1.2 Part of Academia

In the earliest days of the Internet, technical expertise was largely concentrated in universities and research institutions. This accident of history has meant that several ccTLD registries are still part of academia, typically an offshoot of a Computer Science department or the country's academic network. These types of registries can suffer from the same sorts of difficulties as a registry operated directly by the government. Furthermore, the priorities of academia can be very different from those of industry. This can mean such registries may not be as responsive to the needs of the wider community of Internet users as they could be. Stakeholders may have little influence over registry policies.

4.1.3 Independent, externally regulated

In this model, the ccTLD registry is independent. It is not a part of government or a commercial enterprise. The usual types of legal construct for this would be a charitable foundation or non-profit membership association. Membership of the registry is open to the obvious stakeholders: registrars, user groups, internet service providers, trade associations and government. The members elect a management board and help the registry shape its policies. However government, perhaps in the form of a regulator, has direct involvement in policy formation.

Government involvement could be exercised in two ways. Policies developed inside the registry could require government or regulatory consent. The other approach is that the Administration initiates a registry policy that is required for compliance with the government's wider public policy ambitions. Both approaches are likely to mean that government has a high degree of control over the registry's activities and may be too closely involved in matters of technical or administrative detail.

4.1.4 Independent, self-regulated

This model is essentially the same as the externally regulated one above. Once again the ccTLD registry is independent. It is not a part of government or a commercial enterprise. The usual types of legal construct for this would be a charitable foundation or non-profit membership association. Membership of the registry is open to the obvious stakeholders: registrars, user groups, internet service providers, trade associations and government. As before, the members elect a management board and help the registry shape its policies.

However government does not get directly involved in registry policy-making, much of which is about matters of technical detail. This means that the registry can be very responsive to changes in the industry and to local circumstances. It is generally found that bottom-up, consensus driven policy making is the most effective governance mechanism for Internet organisations.

With a self-regulating ccTLD registry, government control and influence is more discreet. An Administration could decide to recognise the ccTLD registry as the organisation responsible for overseeing the ccTLD and the domain names registered in it. This would probably be done through a contract or a formal Memorandum of Understanding that defined the scope and terms of reference for the registry. Provided it stayed within that remit, the registry would be left to its own devices. In essence, government delegates management of the registry but could still take an active role in the registry's policy making activities.

Government could have observer status in the registry's governance structure but would still be able to intervene if the broad public interests were not being addressed. From a practical perspective, government would retain administrative control over the ccTLD while technical control rests with the registry. If the registry does not follow the government's or regulator's wishes, it could have its recognition withdrawn. The Administration would then find some other entity or governance model that was in line with its public policy goals. In this model, the Administration or regulator would probably be the Sponsoring Organisation for the ccTLD so that it could intervene if the registry got into difficulties or was not meeting national policy goals.

4.1.5 Outsourced

Some countries have outsourced the operation of their ccTLD registry to one of the companies which provides this as a service. This can be done for pragmatic reasons, for example to rely on the infrastructure, technical expertise and the registrar relationships of the registry operator that far exceed local capabilities. Sometimes it is to benefit from the business capabilities of the registry operator. A share of the revenue from the sale of `.tv` domain names is a significant part of Tuvalu's income. Verisign, the operator of the `.tv` ccTLD registry, is skilled at promoting that TLD to the world's television industry. The Tuvalu government would not be able to do that as effectively.

The main advantage of outsourcing registry operations is that someone else has responsibility for the day-to-day running of the registry. The level of local expertise is less important because the registry operator already has the necessary engineers and business managers. Established registry operators such as Afilias, Neustar and Verisign will have well-engineered, robust systems and a global presence that are well beyond the capabilities of even the biggest ccTLD registries. In addition, registry contracts can be arranged for a fixed length of time, typically 5 or 10 years. This can ensure the registry operator provides good service and allow the Administration or ccTLD registry to get competitive tenders whenever the contract comes up for renewal.

However there are disadvantages to outsourcing. The first is that it does not nurture local Internet business or expertise: the registry operator has no need for these. The next issue is that preparing an RFP for registry operations is difficult. It will also be necessary for the Administration or ccTLD registry to have the technical and legal expertise to have continuing oversight of the contract with the registry operator. Changes to local policies could require changes to the registry operator contract. Another potential drawback is that the registry operator may not be responsive enough to local needs. The concerns of one comparatively small ccTLD registry may be less important to the registry operator than the other TLD registries in their portfolio that generate the most revenue or have the highest profile. Finally, an outsourced registry may not have a good understanding of local business practices, social or cultural norms and language.

4.2 Operational structure

There are a number of ways in which a TLD registry can be operated. Very small registries that have low registrations are typically operated by hand. The level of business does not merit anything more than that and could not justify the investment that would be needed for a more complex environment. TLD registries operating in this way typically have some hundreds of domain names under management (or less) and perhaps one or two registration transactions each day.

There are a number of TLD registries which operate an integrated service. In these the registry does more than maintain a register of domain names and implement a set of policies. It also deals with registrants: the people and organisations who wish to register domain names. These registries have higher overheads because they have a direct relationship with every registrar, creating an extra load for customer support, billing and so on. Prices to registrants tend to be higher in these types of registries because there is no competition. Since every registry is by definition a monopoly — there can only be one registry for a TLD — any other services the registry provides is likely to prevent others from offering those additional services.

These models tend to be found in highly regulated jurisdictions. Nations that have a deregulated or light touch regulatory environment generally avoid these types of registries because of the anti-competitive markets that tend to result.

Many registries operate a registry-registrar model. This keeps the monopoly function to a minimum and creates the greatest potential for competition and innovation. In this model, the registry just maintains a register of domain names according to locally defined policy. It will usually be responsible for the operation of the TLD’s whois and DNS servers. However registrants do not have a direct relationship with the registry. Instead they interact with the registry through agents called registrars. Registrants pay registrars who in turn pay the registry. Registration requests and updates follow the same path. The registrar gathers the details from the registrant and submits a request to the registry. Figure 1 shows the general idea.

In the conventional registry-registrar model, the registry’s customer support and business procedures are simplified. It is dealing with tens of registrars instead of potentially many thousands of registrants. The registry’s customers are the registrars and they should not need the same level or type of support as the general public. Registrars can provide customer support to registrants who can choose registrars based on factors such as price, quality of support, additional services and so on. It is likely that if this model is followed, local Internet Service Providers would be able to offer domain name registration services to supplement their usual portfolio of Internet connectivity, email and web hosting services.

The conventional registry-registrar model does have some drawbacks. For example, the extra layer of indirection creates more complexity. Contracts need to be arranged with registrars along with any terms and conditions that the registry applies to registrants. Competition between registrars will also need to be monitored by the registry: for example to ensure that registrants are able to switch between registrars without losing their registered domain names or incurring excessive costs.

A ccTLD registry can usually be administered by hand for its initial phase of operations. There will be few registrations, so it is likely there is no need for anything more sophisticated. Better registry management procedures can be gradually introduced as the volume of registrations grows and the level of domain name expertise increases. At some point automation will be needed.

It may be that in the earliest stages of the registry there are no registrars at all: the market has still to emerge. In that case, some sort of web-based facility could be the simplest way for registering domain names through an integrated registry-registrar system. Even if this approach is taken, it would be prudent to design the registry’s systems and processes so that these two roles could be separated at a later date. Section 1.2.7 of Annex C provides additional details about the potential complications of intermingling registry and registrar roles.

There are good reasons why it would be advisable to keep these roles apart. This would allow the local Internet community to establish registrar businesses. From a government perspective, that would encourage competition and stimulate the Internet service business sector nationally. That in turn could also help nurture local Internet expertise. Since every registry is by definition a monopoly — there can only be one registry for a ccTLD — any other services the registry provides is likely to raise barriers to entry and may well discourage others from offering those additional services. This could create problems for local Internet service providers who may want to be able to offer domain name registration services in addition to their usual portfolio of Internet connectivity, email services and web hosting.

4.3 Name Space Structuring

Decisions will also need to be taken about how the ccTLD name space is organised and who or what is allowed to register domain names in it. These are discussed in more detail in Section 6 of this document and in Section 3 of Annex C. In outline, there are two commonly used models: flat and hierarchical. It is also possible to combine these approaches. However a hybrid model which uses both models is not common. Eligibility criteria — determining who gets to register names in which parts of the name space — will usually suggest which of these possibilities is most appropriate.

In the flat model, names are registered directly under the TLD: `example.`*`ccTLD`* for instance. Apart from any reserved names, there is usually no restriction on which names can be registered or who is allowed to register them. Names get registered on a first-come, first served basis. This kind of set-up is simple to understand and administer. The registry only has to implement a single process and policy which everyone has to follow. This model is used by almost all gTLD and a number of ccTLD registries, including `.com`, `.nl` and `.de`. Registrars and end users prefer the simplicity and transparency of the flat model.

The hierarchical model uses a number of labels at the second level to address specific communities or interest groups. The ccTLD registries in Kenya, South Africa and Uganda are examples of this approach. The usual convention is to mimic the structure used by the Internet root zone: `edu` for educational establishments, `com` for commercial organisations, `mil` for the military and so on. Some ccTLDs, notably the UK and New Zealand, use a different convention – `ac` for academic community, `co` for commerce, etc. From a DNS perspective, these differences don't matter.

When the hierarchical model is used, parts of the name space are set aside for specific purposes. The registry has to see that registrations match the appropriate criteria for each part of the name space. Alternatively, the registry might delegate parts of the name space to other organisations who then take responsibility for the registrations that take place there.

This usually means more complexity for the registry as different rules apply to different parts of the name space and extra checking may be necessary. For instance the registry may have to check that requests for names under `gov.`*`ccTLD`* come from authorised officials in government departments or that registrations in `edu.`*`ccTLD`* are only available to academic institutions in the country. Names under `com.`*`ccTLD`* could be offered to commercial organisations in the country on a first-come, first-served basis or under some other terms.

A small number of ccTLD registries use the hybrid approach, notably `.jp` (Japan) and `.us` (USA). Here, labels at the second-level have been set aside for specific purposes or communities: academia, commercial organisations, even individuals and geographic regions. Registrations for names like `example.jp` are handled on a first-come, first-served basis and are usually available to anyone anywhere. In `.us`, the two-letter abbreviations for each state are used at the second level: `example.ca.us` would presumably be some entity in California. In addition names can also be registered directly at the second level, provided those names are not reserved of course.

Decisions on how to structure a ccTLD's name space needs careful consideration. Once that structure is in use, it will be very difficult to change it. Many factors may need to be analysed along with the wishes of the Administration and the needs of the local Internet community. These include set-up and running costs, ease of implementation, revenue opportunities, engagement with foreign companies, available registry resources, nurturing inwards investment, and cultural or business compatibility with the rest of the Internet.

Further criteria could include the terms under which registrations are made. For instance, anyone registering a domain name under, say, `com.`*`ccTLD`* may need to demonstrate that they have already registered that name at a recognised trade mark registry or registry of company names. These sorts of conditions can be applied to reduce the likelihood of cybersquatting: registering domain names that should "belong" to another party. On the other hand a simple policy of first-come, first served could encourage a market in domain names that may boost the country's Internet business sector.

4.4 Registry Business Model

The Administration should consider what levels of fees are appropriate for initial registry operations and who these will be applied to. Once the registry has become operational, the Administration will need to establish some means of reviewing the registry's fees and cost base. It may also need to develop a mechanism for consulting the public on what fees are appropriate to the prevailing operating environment. If the registry operates on a for-profit basis, government should have some way of regulating the registry so that profits are reasonable and not exploited for unfair competition.

A two tier approach to pricing may be worth considering. Registrants based in the country might be charged registration fees in keeping with the local economy, especially if the registration requests come from individuals. Higher fees in line with the usual wholesale price of established TLDs — typically $5-7 per name per year — could be charged to registrants based overseas, assuming such registrations are permitted.

Even higher fees may be charged if there are additional restrictions on registrations or extra burdens on the registry. However these can be unpopular and may be counterproductive. For example, the Irish ccTLD registry charges high prices compared to other European ccTLDs. It justifies those higher fees because of the level of checking they carry out when processing registrations to ensure the registrant has a genuine affiliation with Ireland. Segments of the Irish market do not approve of this approach and claim that the high registration fees are a deterrent to the Irish domain name industry. It is likely that similar complaints will occur if the fees for registrations in the ccTLD are considered expensive.

4.4.1 Managed Registry Model

Several small ccTLD registries use a managed model. Some of these approaches mean there are no registrars. In others, the registry applies many checks to domain name registration requests. These checks tend to be well-intentioned but misguided attempts to regulate the local domain name market or to prevent impostors from registering domain names that should belong to others: cybersquatting.

In the short term, this model can be made to work. In the longer term, these models are usually not sustainable because they are inherently anti-competitive. Firstly, there is often no opportunity for a market in registration services to develop because the registry does it all. Secondly, the registry will usually have a free hand to set prices, effectively rigging the ccTLD's domain name market. Third, these models artificially suppress or constrain the local demand for domain names. Finally, there is generally no possibility of trading or selling domain names. These factors can mean that local Internet users choose to register names in other TLDs instead of their ccTLD.

Many ccTLD registries operated strict checks on registration requests to deter cybersquatting and other unacceptable behaviour. These registries would allow registrations under narrowly defined categories: limited companies, government departments, academic institutions and so on. These models did not scale. Unless requests for new registration categories were rejected — personal names, unincorporated organisations, etc. — too many inconsistencies arose. Registrants, resellers and registrars exploited these inconsistencies to acquire "valuable" domain names for speculative purposes. Strict checking means extra overheads such as submitting paperwork to prove a registrant is entitled to register a domain name. This not only adds cost, but is a further deterrent to domain name registrations and the establishment of a thriving registrar sector in the local domain name business.

In general these rule-based registration systems become progressively more complex until they finally implode. This has been the experience of many European ccTLD registries that started out with a managed registry model. Once these became intractable, the registries were compelled to adopt an unmanaged system with open registration.

Despite these issues a few small European countries, notably Norway and Ireland, appear to be quite content with a managed ccTLD registry that, broadly speaking, restricts domain name registrations to citizens and registered companies of that country.

5 Technical Implementation of a ccTLD Registry

There are a large number of technical considerations that are involved in establishing a TLD registry. These include factors such as choice of hardware and software; network engineering, systems architecture; software engineering and management; configuration of servers; choice of interfaces; technical specifications; security policy; service levels and so on. There are also many practical issues to consider too. For any new and growing organisation, some form of business plan is needed: staffing, organisational structure, outreach, training and of course financial planning. Although these factors are discussed in more detail below, they are intended to just provide guidance about what needs to be investigated. Decisions about many of these subjects will require careful analysis and consultation that are beyond the scope of this document.

5.1 Location

If the Administration decides that its ccTLD registry is to be operated and run locally and follow national law or regulation, the obvious consequence of that decision will be that the registry should be based in the country concerned. However this may not always be practically possible because of the current state of the country's communications infrastructure and other necessary resources. It would be inadvisable to establish a registry in an environment where Internet connectivity is inadequate or if the electricity supply was unreliable. Even if the underlying infrastructure is stable enough, local IT skills may not have the level of experience and knowledge to operate a registry. These are always hard to find. Once suitably qualified staff is available, the registry should of course be established close to most of its expected users and key locations for the country's communications infrastructure.

From a practical perspective, it may be best to first establish the ccTLD registry overseas and train the registry staff there if the local infrastructure and resources are unstable. Once a critical mass has been reached and Internet connectivity is at a suitable level, the registry operation could then be relocated.

5.2 DNS Service

At least one name server for the ccTLD should be installed in the nation once it is practically feasible to do so. Even if the underlying communications infrastructure is unreliable, providing at least one name server for the ccTLD in the country would have enormous symbolic significance. It would demonstrate to the local population and the wider world that the nation was fully engaged with the Internet and determined to play an active part in its future. It would also help to build up the experience and expertise of the country's network engineers. They would learn how to configure and operate core Internet infrastructure — name servers, web servers, firewalls, routers, etc. — as well as running the ccTLD registry.

It should be understood that the DNS has been designed to be resilient to problems caused by temporary failures in name servers and network links. Provided there is sufficient redundancy and reliable DNS service is available elsewhere, the short-term loss of one name server will have a negligible operational impact. If one name server fails for some reason DNS lookups will automatically go to another, hopefully more reliable, name server. In that respect, any name server for the ccTLD that was located in the country would only cause negligible operational difficulties to the rest of the Internet if there were problems with the national communications infrastructure.

The wish to install all of the name servers for a ccTLD inside the country is a commonly held misconception. Superficially this appears attractive from the perspective of control: all the country's ccTLD name servers are under the jurisdiction of the Administration and therefore subject to national law. It may also appear attractive because the ccTLD's name servers are close to the local users who therefore get better service. These are flawed arguments. The Internet's topology does not reflect national boundaries: traffic between two regions in a country can often be routed via an Internet exchange in another country! So name servers that are located at core Internet exchange points will usually be closer in network terms — hop count, round-trip times, etc. — than arbitrary locations within the same city or region. It should also be remembered that DNS lookups for the ccTLD will come from all over the world, not just from within the country. Therefore name servers for the ccTLD should be available at optimal locations for the global Internet community and not just for the local users. Furthermore, installing all the name servers in the same geographic area may unnecessarily introduce single points of failure. Finally suitable levels of control over externally operated name servers can always be achieved through contracts with the providers of DNS service.

RFC 2182 *Selection and Operation of Secondary DNS Servers* provides some general guidance on locating slave (secondary) DNS servers. To eliminate single points of failure, these should be in physically separate locations on different networks provided by different ISPs or Internet connectivity providers. This should ensure that network faults or routing problems will not result in all the ccTLD name servers becoming unreachable, which would effectively cause the country to “fall off’ the Internet. Similarly, using different geographical locations offers protection from outages caused by natural disasters or hazards such as a computer room fire. The obvious locations for important infrastructure name servers are Internet exchange points. These provide good national and regional connectivity, diversity of bandwidth providers and a variety of international and intercontinental links. These facilities are also typically secured from unauthorised physical access. Backup power supplies and generators are usually provided, ensuring continuity of electricity supply. Placing name servers at these locations also means they tend to be very close in network terms to the end users.

Service Levels should be defined for the operation and administration of these name servers. This should provide guarantees on uptime, numbers of queries handled, response times to problems, fault escalation procedures, incident handling, change windows, security operations and so on. ICANN’s published Cross-Network Nameserver Performance Requirements (CNNP) for gTLD operators would be a good starting point for defining DNS Service Levels. Further guidance could come from the many ITTs and Requests for Proposals (RFPs) which have been issued by TLD operators and others for DNS hosting services.

Of course any Service Level Agreements should also take account of prevailing local circumstances that may have an impact on service levels that can reasonably be expected. For instance it would be unreasonable to require a name server which has been physically located in a country with weak telecommunications infrastructure to match the performance levels of a name server that is installed in a major European or American Internet exchange. There would be an obvious disparity in factors such as the reliability of power supplies, bandwidth availability and the quality of Internet connectivity.

5.3 Whois Service

TLD registries generally operate a whois service. This is complementary to DNS service and is a normal part of registry operations. The whois service provides a simple lookup mechanism which returns information about registered domain names. The sort of information that is returned includes the name of the entity which registered the domain name; postal, phone and email details for administrative and technical contacts of the domain; the name of any registrar (if any); and the date when the name was registered and when it is due to expire. The ccTLD registry will need to develop a whois policy to decide what data from the registry database is made available through this service and how or if access to that data gets controlled.

Some registrars and most domain name speculators swamp the registry’s whois servers with queries to check for domain name registrations which are about to expire or have not been renewed. They then re-register the names and try to sell them back to the original owner. This kind of data mining activity often overwhelms a registry’s whois servers. Law enforcement agencies and Intellectual Property lawyers are very strong advocates of whois service since they like to be able to use the data returned from whois systems to help with civil and criminal investigations. Other special interest groups approach whois from an opposite perspective claiming that providing registrant data in this way violates privacy. Providing a whois service that satisfies the needs of these contradictory demands is very difficult.

5.4 Platforms and Software

It is not possible to buy software packages for registry operations. A small number of companies offer registry services. These are built on top of systems and software which have been designed and built by those companies. In other cases, ccTLD registries have developed their own software for managing the registry database and its related systems. These are usually so tightly coupled to the registry’s policies and procedures that they are hard to adapt or install at another registry. The effort to do that can be as much as developing a registry system from scratch.

When starting from scratch a ccTLD registry can be administered by hand for its initial operations. Scripts and database software can be deployed as the volume of registrations grows to a point where automation is needed. This would probably coincide with the introduction of a conventional registry-registrar model where the registrars use an EPP interface.

Much of the software used for registry operations is written in scripting languages such as Perl and PHP, typically building on the open-source toolkits and libraries that are available for these languages. Registries tend to base their customised scripts and applications around open-source software. This means that UNIX- and Linux-based systems are the overwhelming choice for registries. Extensive use is made of open-source software, notably the BIND DNS implementation which is used by almost every TLD registry and DNS service provider. Registries generally develop custom scripts to generate DNS zone files as well as configuration files for name servers and whois servers. These scripts are inevitably coupled to the registry's internal processes and procedures.

If it is considered that building and running the ccTLD registry locally is too ambitious, there are essentially two options. One would be to enter into a service contract with one of the companies that specialise in providing registry services. This approach has been taken by most of the gTLDs that have been created by ICANN. Few of these gTLD registries actually build or operate their own registry systems. The second approach would be to get assistance from an existing ccTLD registry. Many of these are non-profit organisations and they may be willing to make their registry software available or train staff from another non-profit ccTLD registry in how to use that software.

5.5 Expertise And Staffing

Section 2 of Annex C, Country Code TLD Best Current Practices, provides some guidance on the skill sets needed to run a ccTLD registry. Technical and Administrative points of contact should be identified. These will interact with their peers at other TLD registries as well as with ICANN and other industry bodies. For large registries, these responsibilities can be full-time jobs in their own right. At small registries, these roles can be combined.

Graduate-level engineering staff will be needed to operate the registry and look after its systems. If registry operations are outsourced, engineering staff will still be needed to monitor the service provided by the outsource partner and to provide technical liaison. Practical experience of managing DNS servers is a critical requirement. Hands-on experience with EPP or whois — presumably gained at another TLD registry — would be desirable. Relevant programming skills are essential, as is a background in using and administering UNIX- or Linux-based systems. Web expertise, both in managing and configuring web servers as well as in web site design, would be very desirable. Strong experience in internet network administration is also recommended, especially in configuring and managing firewalls or routers. A background in system and network security, databases audit trails and change management would also be useful. Excellent English language skills will be essential for all engineering and management positions in the registry because English is the *de facto* language for Internet governance and technical matters.

At some point, the registry will need to employ customer support staff. Eventually the usual management structure will be required; a chief executive, an accountant, a lawyer, technical manager or systems architect, office administrators, secretaries and so on. For smaller registries, the usual guideline is one full-time employee for every 2,000-5,000 registrations. In other words, if there are 30,000 registrations, the registry is likely to need somewhere between 6-15 staff. Once registrations reach the order of 25-30,000 economies of scale begin to take effect. The registry will have become more automated by this point so the number of staff will not grow linearly with the number of domain name registrations. The largest ccTLD registries each manage 5-10 million registrations with 100-150 employees.

5.6 Interfaces

If a registry is being established from scratch, it would be advisable to use a simple registrar interface, say text-based email templates, for the initial phase of operations. The registry could then develop more sophisticated solutions as demand and expertise grows. It may be that in the earliest stages of a new ccTLD registry there are no registrars at all. In that case, a web-based mechanism might well be the simplest way for registering domain names through a combined registry-registrar system. Even if this approach is taken, it would be prudent to design the registry's systems and processes so that these two roles could be separated later. Section 1.2.7 of Annex C provides additional details about the potential complications of intermingling registry and registrar roles.

There are good reasons why it would be advisable for a ccTLD to keep these roles apart. This would help allow the local community to establish registrar businesses and, from a government perspective, encourage competition. It would also stimulate the indigenous Internet sector. Since every registry is by definition a monopoly – there can only be one registry for a ccTLD – any other services the registry provides is likely to raise barriers to entry and may well discourage others from offering those additional services.

EPP, the Extensible Provisioning Protocol, is the preferred interface for transactions between a registrar and a registry. Although EPP is the *de facto* standard, there are others. An older protocol, RRP, is still used sometimes even though it is effectively obsolete. Some registries offer web-based interfaces. Others provide interfaces based on email-based templates. It is also not uncommon for registries to provide a combination of these interfaces. Sometimes registrars will refuse to replace or upgrade their systems and processes, forcing the registry to maintain legacy interfaces and infrastructure indefinitely.

EPP is a complex protocol. Developing an implementation and test suite for EPP is a substantial undertaking. Registries using EPP need to provide toolkits so that registrars can communicate with them. Sometimes registries need to provide testbeds too. Registrars will have EPP client software but this will need to be adapted for each registry they interact with because the schemas and templates for each registry are different. It would be advisable for the registry to only deploy EPP once the local Internet community has matured and sufficient expertise is available. However it is recommended that the registry systems and processes are designed from the outset to accommodate a variety of technical interfaces, including EPP.

In addition to technical interfaces, a ccTLD registry will need to interact with a number of external organisations. The most obvious of these will be the Administration and any relevant regulatory agencies. This will probably involve some sort of legal framework, perhaps a contract or a Memorandum of Understanding. Describing that framework is out of scope for this report since this is a national matter and it is not known what regulatory environment, if any, is likely to apply to a ccTLD registry.

The registry will be expected to engage with the local Internet community and publicise its activities. These outreach efforts could include public meetings, workshops with business groups, liaison with academia and so on. There should probably be an education programme: helping end users, engineers and government officials to understand how the Internet works as well as how the country's Internet infrastructure is operated and governed. Finally, staff from the ccTLD registry should get involved in the associations and industry fora that deal with Internet matters. These would include institutions such as ICANN, IGF, IETF, CENTR, AFRINIC and AFTLD.

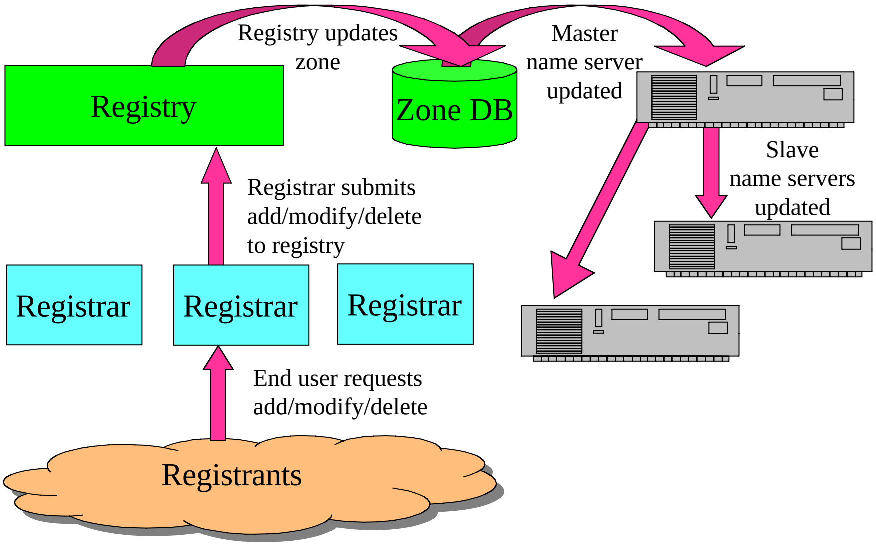
5.7 Routine Registry Operations

At a minimum, an Administration will need to retain administrative control over its ccTLD registry. This is central to preserving the integrity of the country's name space and for ensuring that the registry operates in accordance with the Administration's public policy goals.

It may also decide to enter into an agreement with ICANN. Some ccTLD registries and governments or regulators have formalised their relationships with ICANN. Many have not. There is no requirement or obligation to do so. Most of these agreements are simple: a straightforward exchange of letters or a statement of mutual recognition. Details of these agreements can be found on the ICANN web site at http://www.icann.org/cctlds/agreements.html.

Operation of the registry itself is in principle straightforward. Typically information supplied by registrants is entered into a database. At regular intervals the database is scanned by an SQL script to produce a DNS zone file. This is then checked, transferred to the master server and loaded. The DNS protocol then ensures that slave servers get an updated copy of the zone. Figure 2 shows the typical data flows and the entities who are involved.

Figure 2 – Entities and Data Flows in a Conventional TLD Registry


Registry updates zone
Master name server updated
Registry
Zone DB
Slave name servers updated
Registrar submits add/modify/delete to registry
Registrar
Registrar
Registrar
End user requests add/modify/delete
Registrants

The obvious criteria for running mission-critical services should be applied. The systems should be set up with adequate protection to prevent unauthorised access. This should ensure that the integrity of the system software can be maintained. It is even more important that the integrity of the data served by those systems cannot be compromised. Strict access controls will be necessary, perhaps based on public-key encryption and/or X.509 certificates. Change control procedures will also need to be developed and enforced, backed up by extensive audit trails and a trouble ticketing system.

Strict security and operating procedures must be defined and deployed for the registry, especially regarding change control and audit trails. The registry database defines the ccTLD name space. In reality, the registry is the ccTLD name space. It contains the data used to generate the ccTLD zone file, configure the name servers, generate invoices, maintain registration data and so on. If the registry is compromised or corrupted in any way, the integrity of the country's Internet presence is lost.

In this sense the registry is even more important than a ccTLD's name servers. The registry systems should be protected by firewalls and strict access controls. It may even be necessary to isolate them from the Internet and use some out of band mechanism for getting zone data to the name servers from the registry. As a general rule, commercial registry providers use this approach. Registrars get tightly controlled access to an EPP channel which allows them to send transactions to a server which is the only resource permitted to change the registry database because it has exclusive write access to the database server.

The registry operator must monitor the operation of its name server infrastructure. One function is to check that the name servers are running correctly with accurate and consistent data. A second consideration is checking for procedural problems such as name servers that are not complying with agreed service level commitments. Problem reporting and escalation procedures will need to be defined. The name servers should be configured so that their exposure to attacks such as cache poisoning and spoofing are minimised. It is beyond the scope of this document to describe these defensive measures in depth here.

Because of the likely global nature of the registry, it may have to run 24x7x365, even though the registry itself may not be mission critical. If the registry was not available, changes to registrations and delegations will not be possible. This would be inconvenient although it would not affect the operation of the ccTLD's DNS infrastructure. Careful consideration will need to be applied to the selection criteria and requirements for service level availability of the registry, especially if it is outsourced. These would include factors like uptime, response time to requests, time to propagate changes to the DNS infrastructure and so on. If operation of the registry is to be outsourced, a Service Level Agreement will need to be defined with the outsourcing provider. ICANN's requirements on gTLD operators give a good foundation for defining service levels for any outsourced registry services provider.

It may appear that a 24x7x365 requirement for the registry is excessive and unreasonable. This could well be the case, especially in the early days of registry operations when the volume of domain name registrations and frequency of support requests from registrars are unlikely to justify that level of commitment. It may be reasonable to start off with the registry operating using conventional office hours and then to expand operations as the registration volumes and revenue increase. However even if an “office hours” registry is adequate for processing registrations, there will be a need for round-the-clock monitoring of the ccTLD’s name servers. This could be outsourced and perhaps coupled to an on-call rota for the registry’s engineering staff.

The systems running the name servers should be configured to run the barest minimum of network services. The advice in RFC 2870 — *Root Name Server Operational Requirements* — provides general guidance about the configuration and operation of the systems running important name servers. Apart from the name server itself, each system should run time synchronisation software typically `ntpd`, some monitoring software and a cryptographically secure remote access mechanism, such as the Secure Shell, `sshd`. The monitoring software should ensure that name server operations staff is alerted to issues as they arise. A similar approach should apply to the other registry systems: any whois and web servers for instance.

No other services should run on these systems. There are several reasons for this requirement. The first is simplicity. The fewer subsystems that are in use, the fewer things there are to go wrong. This also means system administration is almost eliminated which reduces the need to alter configuration files, apply patches and so on. A second reason is reliability. In general computer systems that do not need regular intervention or frequent software maintenance tend to be more reliable. When there are fewer subsystems in use, there are fewer software components that will need to be patched or upgraded. The final reason is security. It is easier to defend against attacks when there are a small number of simple, well-defined services deployed. There are fewer vulnerabilities to exploit because there are fewer subsystems in use and these are unlikely to have complex or subtle interactions between each other.

Accurate time stamps are critical for registry operations, notably for resolving disputes concerning the time when registration requests or transfers were received by the registry. Therefore, `ntpd` is recommended so that each server used by the registry keeps reliable time and all the systems are synchronised with each other. Besides being good administrative practice, accurate timekeeping is also vital for the operation of Secure DNS (DNSSEC) and Transaction Signatures (TSIG) which include timestamps for validating data. Further information about the Network Time Protocol, NTP, can be found at http://www.ntp.org.

The secure shell protocol uses a combination of asymmetric and symmetric cryptosystems. Public key encryption is used to authenticate hosts and users. It is also used by the client and server to select a symmetric encryption algorithm such as DES or IDEA and negotiate the exchange of a session key which is then used to encrypt the data sent over the connection. Passwords are not transmitted in clear text. Details about SSH can be found at http://www.ssh.org.

Open source monitoring software such as MRTG or RRDtool tends to be used to check the status of the name servers and report problems like crashed or hung name server daemons, hardware errors, full file systems and so on. Most TLD registries use these tools as commercial software is not available or cannot be readily adapted to the bespoke needs of registry operations. The MIB for name servers has been deprecated so there is no SNMP support in the DNS. This means it very difficult to integrate name server operations with network management systems. The monitoring tools should perform frequent sanity checks on the data in the DNS: for example verifying that all the name servers are up, answering authoritatively and holding consistent data. It is also possible to buy DNS monitoring services from commercial service providers.

6 Policy Formation for the ccTLD Registry

Apart from implementation of the Administration's public policy objectives, a framework for making policy decisions concerning routine operations of the registry will need to be developed. Provided the broad public interests are addressed — for example compliance with national law, adherence to government policy principles, etc. — these day-to-day activities do not necessarily have to directly involve government. From a government perspective, these registry policy considerations and technical details are unlikely to be of interest. It is of course important that the government monitors these issues and intervenes when necessary.

6.1 Policy Making Body

The usual way this is handled is through some sort of Management Board which oversees the operation of the registry. This Management Board would probably have representatives drawn from stakeholders concerned with the operation of the registry: registrars, internet service providers, user groups, non-governmental organisations, law enforcement agencies, academia, government departments and so on.

The scope of the Management Board would be determined by the Administration: its terms of reference; powers; responsibilities; how members are appointed or selected; the extent of any self-regulation and so on. Responsibilities which could be devolved to the Management Board could include: selection and appointment of a registry operator; negotiating and executing a contract with an organisation providing registry services; producing codes of conduct, contracts and accreditation for registrars and other entities involved in ccTLD domain name registrations; developing acceptable use policies; eligibility criteria for registrations; payment terms and pricing; determining processes and procedures for handling disputes and appeals; technical interfaces; defining national standards for domain names; and the adoption of new DNS and registration technologies. These are described in more detail below.

This structure works rather well and most European ccTLDs operate along these lines. The registry is typically some not-for-profit legal entity — a charitable foundation or membership association — and the Management Board are the directors or trustees of that entity. The senior management of the registry report to this Board and are accountable to it. This also creates a tidy separation between the roles and responsibilities that apply to the operational and supervisory functions.

Sometimes, a two-tier approach is taken. This can arise for a number of reasons. For instance, it may not be possible for government officials to be directors or trustees of an organisation that's not part of the government. If the registry organisation is membership-based, a regulator or government departments might not be eligible to become members because of the organisation's membership criteria. If branches of government are not directly involved in day-to-day interactions with the registry, they may not qualify for membership.

In these kinds of scenarios government and regulatory oversight can be exercised through a second board, usually known as a Policy Board. Typically the Management Board is drawn from the organisation's membership and act as its legal directors with responsibility for running the organisation. The Policy Board can be partly elected by the membership but also has permanent representation from government and any regulatory or statutory bodies. The Policy Board makes recommendations to the Management Board and could have some form of scrutiny over the activities of the Management Board. This kind of structure ensures the required public safeguards are in place from a government and regulatory perspective. Nominet, the registry for `.uk`, uses this type of governance structure and is a good example of its kind.

6.2 Contracts

A registry organisation is likely to have contracts with suppliers: providers of registry services or DNS hosting for example. It will almost certainly have contracts with registrars. These could go into great detail about service levels, payment of fees, technical interfaces and so on. A sample registry-registrar contract is shown for illustrative purposes in Annex E. [This example is the actual contract ICANN requires Afilias, the registry operator of `.info`, to offer to all of its registrars.] The details of these types of agreements are unlikely to be of interest to a government. However government may wish to ensure that these contracts follow general policy principles on topics such as non-discriminatory terms of business, fair competition, consumer confidence, privacy and so on.

Similarly, if the registry is self-regulating, its stakeholders would be free to produce codes of conduct, acceptable use policies, accreditation criteria, develop policy-making processes and other documents or policies concerning routine registry business. These too are unlikely to matter to government as long as public policy is being followed. In this context, the policy-making processes are those of the registry and its stakeholders, not those of the government.

6.3 Usage Policies

Most registries have acceptable use policies and codes of conduct that apply to their customers. These can include obligations to respect privacy, not to harass other users, fair use of registry data and so on. They can also define terms and conditions that are attached to registrations, the responsibilities of all parties, limitations on liability as well as procedures for handling disputes. A good example of this type of agreement is on the web site of Nominet, the UK ccTLD registry: http://www.nominet.org.uk/registrants/aboutdomainnames/legal/terms. There may be specific policies for different users of the registry. For instance, registrars may be obliged to sign contracts and lodge money with the registry.

From time to time, changes to these policies will be necessary. This could happen for operational reasons or because of external factors: a change in the law perhaps or the adoption of new DNS or whois technologies. The registry will need to develop a process for initiating those changes, allowing the community to comment on them, and to inform users before the changed policies or new rules take effect.

If the Administration favours a self-regulating model, the registry would be able to develop new policies and codes of conduct that are appropriate to its community. This too could be an area where direct government involvement is not needed. However, if the registry is a branch of government or regulated, government officials will be involved in the day-to-day formation of registry policy and processes. These could be an undesirable burden.

6.4 Eligibility Criteria

Some registries apply checks for registration requests and renewals. Checks can be technical in nature: for instance ensuring that the DNS servers for the domain name are operating properly. Other checks are administrative: verifying the identity of the registrant or ensuring that the company actually exists when a registration request is made for that company. As part of an outline set of registry policies, the Administration should consider which checks, if any, should be performed by its ccTLD registry. Clearly some checks will be cheap and quick because they can be done by computer. Others could be time-consuming and expensive because human effort is involved. There are trade-offs to be made here between what is desirable from operational and policy perspectives and what can be achieved with the resources available to the registry and, by implication, the fees that can be recovered from registrants.

It may be worthwhile having different criteria and checks for different parts of the ccTLD name space. For instance, the registry could take reasonable measures to ensure that only companies registered and based in the country were allowed to register domain names under `.com.`*`ccTLD`*. Companies might be prepared to pay extra for those registrations if the public believes that domain names in `.com.`*`ccTLD`* are more trustworthy than those offered by registries that do not check registrations.

Other examples of eligibility criteria could apply to how parts of the ccTLD name space are assigned to sections of society and the local Internet community. Any domain names under `.gov.`*`ccTLD`* would no doubt belong to parts of the government and the government will decide which names get registered there and who is allowed to register those names. Domains in `edu.`*`ccTLD`* could be assigned to academic institutions on the authority of the Ministry of Education. Similar types of criteria could be applied to other parts of the name space. This should be determined by a process of consultation involving the Administration, the ccTLD registry, representatives of the local Internet community and other stakeholders.

6.5 Pricing

Although the Administration is expected to determine the initial fee structure charged by the registry, there could be a need to adjust those fees based on local circumstances and eligibility criteria. These amendments could take account of factors such as the registry's profit margin and/or balance sheet, the prices that the local market can bear, fees charged by "competitor" registries and so on.

Perhaps the main regulatory concern here for the government or a regulator is that fees get set through a transparent process that has general acceptance by the users of the registry and that the level of fees is reasonable. If this is the case, the registry's pricing policy will be essentially self-regulating. However as mentioned before, the Administration will need to have some way of ensuring that the registry, which is after all a monopoly, operates in the broad public interest and in accordance with the Administration's policy objectives.

6.6 Disputes and appeals

Complaints can arise about all sorts of issues. These include registry fees; ownership or transfer of a domain name; bad faith registrations; malicious behaviour by registrars and registrants; violations of any codes of conduct or acceptable use policies; accreditation issues; cybersquatting and phishing; and abuse of the registry's systems or procedures. It is important that the registry remains strictly neutral in these disputes — it may be a party to them! — and does not get directly involved in resolving them.

A well-run registry will need to develop processes and mechanisms for handling disputes and appeals. These can deal with the mechanics of complaints: how they are handled, who is allowed to make a complaint and how they are resolved. An appeals mechanism may also be required. Typically an independent *ad-hoc* panel is appointed and hears evidence from parties concerned with the dispute. This can usually be co-ordinated by the registry without the need for lawyers or formal legal proceedings. Once the internal disputes procedure is exhausted, the parties may still have the option of going to arbitration or the courts.

An excellent resource for information on dispute resolution policies is provided on ICANN's web site at http://www.icann.org/udrp. This URL contains an impressive set of dispute resolution policies covering almost every area of aspect of domain name usage. These could be used to guide the development of the ccTLD registry's dispute handling policies.

Some types of complaints are best handled by other parties. ICANN has developed a well established and widely accepted process called UDRP (Uniform Dispute Resolution Policy) for handling disputes where two or more organisations claim ownership of the same domain name. These complaints usually arise because of competing trade marks and an expert opinion is needed to determine which trade mark holder has the strongest entitlement to register the domain name. No registry has the expertise to make these sorts of decisions or can risk the legal consequences of making an incorrect determination. It would be prudent for the registry to rely on UDRP facilities to handle these kinds of disputes. This will probably mean reaching an understanding with WIPO, the World Intellectual Property Organisation, which is the most common choice for handling these types of complaints.

A quick solution would be to adapt the dispute resolution processes of an established, comparable ccTLD registry. Quite a few European ccTLD registries offer Alternate Dispute Resolution (ADR) because local stakeholders are reluctant to use UDRP because of the cost and time. Details of a good example of an ADR can be found at http://www.adreu.eurid.eu. This web site contains a complete description of the ADR used by the `.eu` ccTLD registry.

Procedures for handling disputes should be transparent and fair. This will require the registry to develop and publish these processes. It may be advisable to get agreement from registrars and registrants that they agree to these processes, perhaps by including these in the registry's general terms of business and/or acceptable use policies. As before, government does not need to be directly involved in resolving disputes and complaints. It may be sufficient that the Administration ensures that there is a fair and transparent complaint handling procedure in place at the registry.

6.7 Interfaces

Decisions will need to be taken about the technical interfaces that will be offered. These could include choices of EPP version; changes to EPP schemas and templates; deployment of new registry-registrar protocols and so on. Discussions and consultations on such matters will be highly technical in nature and will probably be too detailed for government or regulators.

At present, the Extensible Provisioning Protocol, EPP, is the preferred interface for transactions between a registrar and a registry. Although EPP is the *de facto* standard, there are others interfaces. An older protocol, RRP, is still used sometimes even though it is effectively obsolete. Some registries offer web-based interfaces. Others provide interfaces based on email-based templates. It is also not uncommon for registries to provide a combination of these interfaces. Sometimes registrars will refuse to replace or upgrade their systems and processes, forcing the registry to maintain legacy interfaces and infrastructure.

Other types of interface are non-technical in nature. For example the registry may have a requirement to conduct regular public meetings to explain what it does and get comments directly from the local community. In the interests of openness and transparency, the minutes of board meetings and details of the registry's finances could be published. Most registries produce an annual report describing their activities and financial accounts. There is usually at some sort of Annual General Meeting to elect Board members which may also approve the registry's annual report and budget. If the registry is independent of government, there will be a need for some form of agreement or regulatory structure defining how the registry and government officials interact.

6.8 Service levels

The registry should define service levels for the operation of the registry system and its infrastructure of web servers, whois systems and DNS servers. These include uptime, performance, propagation time for changes, throughput and response times. When the registry equipment is operated in-house, these metrics help to manage the registry's operations team. When parts of the registry's infrastructure are outsourced — some DNS servers for instance — these metrics can be incorporated into the contract with the service provider.

If the standard registry-registrar model is followed, the registry will be expected to provide registrars with commitments about the registry's services. These would include information on the availability of the registry system, maintenance windows, response times and problem escalation procedures. It is also common in the domain name business for these commitments to be supported by a system of credits or penalty payments if the registry fails to meet those service levels. Usually the details of these performance levels and credits are included in the registry-registrar agreement. A sample agreement is shown in Annex E. The registry may choose to apply performance metrics to registrars, notably in the area of payments and load on registry infrastructure.

Again, decisions and discussions on such matters will be highly technical in nature and will probably be too detailed for government or regulators. It may be that the Administration would be satisfied that the registry had a reasonable set of service level commitments and was honouring them. In that scenario, government or regulatory intervention would only be needed if the registry was not meeting its obligations.

6.9 Escrow Arrangements

ICANN has contacts with its gTLD operators that require the registry's data to be regularly lodged with an escrow agent. This ensures that in the event of the business failure of a registry, the registrants and other users of the gTLD are protected. The database of the failing registry can be released by the escrow agent to another registry provider. In theory this would allow the gTLD to resume operations. Data escrow may also be useful for business continuity purposes. For instance, if there is a catastrophe at the registry such as a computer room fire, the registry can in principle recover its data from the escrow agent and continue operating from some disaster recovery location.

ICANN has no authority to require ccTLD registries to use an escrow agent. This is a matter for the relevant Sponsoring Organisation and Administration.

An Administration should consider whether its ccTLD registry should escrow its registry database. Some countries have already arranged this facility. The attractions here are obvious. If the ccTLD registry database is escrowed, it will in principle be easier to move registry operations to a new registry provider. Similarly, the registry's processes, procedures and data schemas are likely to be in a standardised form that makes them simpler to transfer. On the other hand, data escrow does increase costs and adds complexity. There should be a wide consultation about the advantages and disadvantages of introducing data escrow at a ccTLD registry. Careful consideration needs to be given to the cost/benefit analysis of these schemes.

6.10 Naming considerations

Many ccTLD registries operate a hierarchical approach using a conventional set of second-level labels: com.*ccTLD*, gov.*ccTLD*, edu.*ccTLD* and so on. Brazil, Kenya and Sudan use this approach. These ccTLD registries sometimes have a logical separation of the registry functions for these second-level labels. For instance, the government's Ministry of Education might have direct administrative control over edu.*ccTLD*, deciding which names schools or universities are allowed to register there, even though the edu.*ccTLD* "registry" is actually operated by the ccTLD registry. Another approach is to assign second-level labels to geographic or administrative regions of the country. The most visible example of this is .us, which has entries for the two-letter codes for each of the 50 states that form the United States of America.

Most end users and registrars prefer a simple, flat name space under the ccTLD, where domain names like example.*ccTLD* can be registered. This naming structure is followed by quite a few countries, most notably by Germany and The Netherlands, two of the biggest registries in the world. A simple structure like this is more likely to be successful at attracting Sunrise and Landrush registrations. These are discussed in more detail later in this document.

Careful attention should be given to Section 3 of Annex C, Country Code Top-Level Domain Guidelines. This contains good advice about structuring a country's TLD name space, the choices that can be made and the advantages and disadvantages of these various approaches. It is almost impossible to restructure a name space once it is in use. Domain name migration is very difficult, error prone and creates many problems with backwards compatibility. The old names tend to remain in address books, search engine databases and business stationery. Therefore it is important to consult widely about how the ccTLD name space is to be organised before making a final decision on this matter. Once that decision has been made and domain names are in use, it may not be feasible to change that decision.

If the Administration decides to adopt a hierarchical name space, it will be necessary to determine which entities and individuals will have administrative control over parts of the name space. For instance, it would probably be an official of a government department that decides which names can be registered under gov.*ccTLD*. That official would be responsible for the process which would be followed when a name is to be registered there. There may also be a need for a technical contact and a process for creating delegations, assuming these were felt worthwhile, if parts of the ccTLD name space were to operated independent of the ccTLD registry. For example edu.*ccTLD* (say) could be delegated by the registry and operated by the Ministry of Education.

A further element of this proposed naming standard could include details of any reserved names. If the Administration has concerns about offensive or obscene names these could also be addressed in this proposed naming standards document. Though instead of compiling a list of offensive names, a more pragmatic approach would be to just define a policy and then take action whenever a domain name is registered that is considered to be offensive.

This naming standards document could also define how or if Internationalised Domain Names are to be handled by the registry.

6.11 Deployment of emerging technologies

The Domain Name System is in a state of continual extension and improvement. New features get added as the protocol is enhanced with new functionality. Changes and new working arrangements are also a feature of the registry business, though these tend to be about process and policy matters rather than technical issues. Every registry will need to track these developments and made decisions about when or if to introduce these.

This too may well be low-level detail that does not need to involve the Administration directly. However it should of course have some influence over the introduction of these features.

In particular there are three prominent emerging DNS technologies that are likely to require attention.

The first of these is Internationalised Domain Names (IDNs). This provides a way of mapping between names in other scripts or alphabets and the restricted set of ASCII characters that can be used for host names: essentially email addresses and URLs. Some TLD registries already offer IDN registrations, notably those serving predominantly Asian communities or countries. At some point it may be desirable for a ccTLD registry to do this: for instance to encourage Internet usage amongst the local population who are uncomfortable with languages and scripts which are based on Latin characters. The core specifications for IDN are defined in RFCs 3490, 3491 and 3492.

The second technology is Secure DNS: DNSSEC. This uses public-key cryptography to generate signatures over data published in the DNS, providing a way for responses from the DNS to be validated and verified. Although protocol development is still under way, deployment of DNSSEC has begun. This technology offers protection from DNS spoofing and phishing attacks. Because of its complexity, extensive consultation and analysis should take place before DNSSEC is introduced. RFCs 4033, 4034 and 4035 describe the current protocol. Further work on the protocol is still under way at the Internet Engineering Task Force, IETF.

The final emerging technology is ENUM, which maps E.164 telephone numbers into domain names. ENUM can be an enabler for next-generation telephony based on Voice over IP (VoIP). It can also be used in conventional telephone networks to provide very efficient solutions for number portability and call routing. Most countries that have deployed ENUM to date have made the incumbent ccTLD registry operator provide the national ENUM registry. The basic ENUM specification is given in RFC 3761, though a number of ENUM-related standards documents have been produced by the ITU and ETSI. If an Administration decides to adopt ENUM, the country's ccTLD registry operator would be an obvious choice to take a prominent role in that activity.

Another very important consideration is the adoption of IP version 6 (IPv6). IPv6 uses 128-bit addressing. Almost all of the Internet is based on IP version 4 (IPv4) which uses 32-bit addresses. If current usage trends and address allocation policies continue, it is estimated that the IPv4 address space will be exhausted in 3-5 years. This means that it would be prudent to plan for deploying IPv6 and operating in an Internet which uses both types of addresses. For a ccTLD registry, this will entail providing IPv6 connectivity to the registry and its related systems: web sites, whois and DNS servers. It is also likely to mean educating the local users about IPv6 and developing a policy on the provision of IPv6-capable name servers for delegations of the ccTLD: i.e. `example.`*`ccTLD`*.

Registry processes and best common practices are also subject to change. Some of these emerge as a result of developments at ICANN. Others arise from industry associations such as CENTR. It will be important for ccTLD registries to track these developments and introduce new registry policies from time to time. Typical issues include business continuity arrangements, risk assessments, data escrow, alterations to registration life-cycles and so on. ICANN has a task force working on whois and a report is due soon, so changes to TLD whois policies and practices are on the horizon. The recent failure of a prominent registrar, RegisterFly, has raised the subject of registrar escrow arrangements and accreditation criteria. These kinds of things will require on-going attention from the ccTLD registry in particular as well as from government and regulatory authorities.

7 LAUNCHING THE CCTLD

Special opportunities may be available if there has been a radical reorganisation of the ccTLD. A change of Sponsoring Organisation or liberalisation of registry policies may open up the ccTLD to a wider public. This may present a unique opportunity to promote the ccTLD globally and raise the profile of the registry. It may also provide the registry with an injection of cash from registrations that could help it become financially self-sufficient in a matter of months. This opportunity can be considered to be analogous to the process for launching a new TLD.

From a technical perspective, this launch process covers aspects such as establishment of the registry and its infrastructure of name servers, whois servers, registrars and support. However a TLD launch involves many other activities. These include outreach, liaison with registrars, marketing and business development. Most TLD launches go through a series of steps according to a timetable. It would be prudent for the Administration to consider this opportunity and, if appropriate, develop such a plan in consultation with the likely stakeholders.

The launch plan could present a number of business opportunities that can yield significant revenue before the registry opens for business to the general public. These possibilities should be explored and due consideration given to how the generated income is used. The revenue could provide a stand-alone registry with sufficient funding to be financially independent and perhaps recover its start-up costs. This model is commonly used with new gTLD launches. Most of their business plans work on the assumption that pre-launch activities bring in enough money to operate the registry until it reaches profitability or break-even point.

There are three distinct phases for these pre-launch opportunities: Sunrise, Landrush and Reserved Names. These are described below. Some TLD launches have used complex multi-phase strategies with varying degrees of success. These are not discussed in detail here. However these options should be considered if and when a launch plan is developed. It should also be underlined that complicated strategies are hard to explain to registrars and consumers, confusing the market. In addition they can create more opportunities for problems and therefore require a very careful cost-benefit analysis.

At the end of these pre-launch activities, the registry enters what is known as General Availability: the point at which it accepts registration requests from the general public or the subset of the public that it is permitted to register domain names.

For all aspects of the launch plan and General Availability, it is important that a good working relationship is established between the registry and the registrars. This is needed at both a technical and administrative level for the obvious reasons. The interfaces and processes need to be well defined, thoroughly tested and clearly understood. National and registry policies should be clearly explained to registrars so that they in turn can pass on that information to their customers, the registrants, and to enable them to act as first-line support to the general public. This is not a role that a registry should take on and many registrars will actively discourage anyway: they generally do not want anyone else interacting with their customers. Establishing a good relationship between the registry and registrars can be mutually beneficial in other ways. For example, joint marketing and outreach programmes could be undertaken. These could be used to increase the visibility of the ccTLD as well as raise general awareness about the registry and its initiatives to nurture the local use of Internet technologies.

7.1 Sunrise

The first component of a TLD launch plan is Sunrise. This gives an opportunity for holders of trademarks, service marks and other intellectual property rights to register domain names before General Availability starts. The registry usually runs the Sunrise in partnership with a Validation Agent (VA). The Validation Agent checks Sunrise applications against national trademark registers and may make some judgement about who has the right to a particular name. Legal liability for any errors made during these decisions generally rests with the VA. Sunrise Validation is a fairly well understood operation and services are available from a number of companies, usually an offshoot of a major accountancy or consulting firm such as Deloittes or KPMG.

Trademark holders are often reluctant participants in Sunrise. However they prefer this to losing control of their Intellectual Property and corporate branding. Sunrise gives them the opportunity to make defensive registrations of their trade marks and company names. This prevents these names going to impostors, saving the trade mark holder from the time and expense of legal action to resolve disputes and reclaim the domain name. A further incentive for defensive registrations is to guard against loss of goodwill or damage to the company's image.

There tend to be two approaches to Sunrise applications. The first is to operate a first-past-the-post system. The registry announces a start date when applications can be accepted. It also sets a closing date, usually 4-6 weeks afterwards. The first valid application for a given name is successful. This approach is popular with registrars because it provides them with extra revenue opportunities. They can sell places in their request queues and trademark holders may make multiple applications for the same names through different registrars. The second approach is to announce start and end dates for applications as before. However no selection is performed until after the closing date. When there are competing requests for the same name — say polo.*ccTLD* — the Validation Agent makes a random choice between the competing trade mark holders: for example the car, clothing, and confectionery companies that have different but equally valid international and national trade marks for "Polo". The first selection that can be validated against an appropriate trade mark registry is successful. A variation on this scheme is to organise an auction when there are competing valid registration requests for the same name. Further information about auctions is given later in this section.

Trade mark holders tend to prefer the second approach as it is generally less expensive and considered to be fairer. However random selection is a form of lottery and this can result in litigation. Neustar, the registry operator for .biz, ran into serious problems when they used random selection for Sunrise applications. The US courts decided this constituted an illegal lottery. This decision ultimately forced Neustar to refund all Sunrise application fees for .biz. It should be noted that even if a Sunrise based on random selection is possible under prevailing national law, this could still result in legal action in the USA because the ccTLD would have been delegated to the Administration by ICANN, a US company subject to US Federal and Californian State Law. Expert legal advice will be necessary before this Sunrise approach could be used.

The success of a Sunrise depends on a number of factors. These include the choice of Validation Agent: some are better than others. The level of promotion and outreach by the VA and registry is also important. This raises awareness amongst the Intellectual Property Rights community and helps them explain the Sunrise to their clients. Some registrars specialise in this activity and their involvement from an early stage is crucial to a successful Sunrise. Pricing is the next most important factor. If Sunrise applications are too expensive there will be fewer applications. The timing is also a key factor. Plenty of notice — six months or more — is needed to allow big companies to prepare and make budgeting decisions. The Sunrise should also be aligned with budget cycles, particularly for US-based companies that generally synchronise their financial year to the calendar year. This means early in the calendar year is a good choice for running a Sunrise, late is not. Assuming of course there was sufficient outreach and promotion for some months before the Sunrise starts. A complex Sunrise application process that is hard to explain or understand will result in a confused market and low uptake.

The volume of Sunrise applications has varied dramatically in recent TLD launches. The .eu TLD had approximately 250,000 successful Sunrise applications. At the other extreme, the .mobi Sunrise only attracted 15,000 successful applications. Tentative discussions suggest a Sunrise for a relaunched ccTLD could possibly generate 20-25,000 applications at a fee of $200 each. If correct, this could raise approximately $5,000,000 which would be expected to be divided equally between the registry and the Validation Agent.

7.2 Landrush

Once the Sunrise application process has closed, the Landrush phase can begin. It should be noted that even though Sunrise applications are no longer possible, the Sunrise process could still be under way. The Validation Agent may well be checking applications and making determinations. However by this time it will be clear to the registry and VA which names have been "reserved" through Sunrise applications. Any remaining names could be made available for Landrush.

Landrush generally operates for a month or so shortly before General Availability of the TLD. Usually names can be registered by anyone during Landrush and the price of Landrush registrations is usually some multiple of the registration fee charged during General Availability. This gives an opportunity for the registry to obtain more money for domain names where the public is prepared to pay a premium price. Typical names that could be sold during Landrush include generic terms like `computer.`*`ccTLD`* or `internet.`*`ccTLD`*. [These are actually poor examples as there will almost certainly be existing trade marks for these terms and it is anticipated that those names would be snapped up during Sunrise.] Landrush registrations are generally made by registrars on a speculative basis. They buy the names in the hope that they can later be sold on to a third party or to sell advertising space on web sites built around the Landrush domain name.

A well-executed Landrush could possibly generate $500,000: perhaps 20,000 applications at a wholesale price of $25 each. In other words, the registry charges $25 for each Landrush registration and does not have to share that revenue with anyone else. Registrars would typically charge their clients twice the wholesale price for a registration. If the registry sets high registration prices at Landrush, this will mean high prices for consumers which will deter registrations. A balance should be struck here between revenue expectations and the retail prices the market will bear. Again, careful cost-benefit decisions have to be made.

It should of course be appreciated that a Landrush phase is unlikely to make commercial sense unless registrants can trade domain names amongst themselves. It is possible that some registrants will always be willing to pay a premium to obtain domain names before they become available to the general public. However if there is no after market in domain names or if the registry's rules for transferring domain names between registrants are too restrictive, there may be little enthusiasm for a Landrush. The value of these names may not be attractive because there is little demand for them and few opportunities to sell these names at a profit by transferring the registrations to another registrant.

7.3 Reserved Names

Lists of reserved or premium names can be compiled and held back from conventional registration. The registry can then make a decision about when and how these names are made available: some sort of auction for example. Strictly speaking, an auction of names can be done at any point. In fact they are usually held after the start of General Availability. By that point, the needs of the Intellectual Property Owners will have been satisfied by the Sunrise Phase. Speculators and traders in domain names would have acquired valuable names during Landrush. Even so, there may still be a pool of valuable names that could be reserved and sold to the highest bidder. The `.mobi` gTLD registry has compiled lists of premium and geographic names that have been held back from general registration and are available for auction.

Besides compiling a list of premium names, there are likely to be other names that the Administration or registry may choose to reserve. These names would not be made available for technical, policy or pragmatic reasons. There are at least three categories of reserved names.

7.3.1 Generally Withheld Names

These are names which are conventionally accepted as being not available for general use. They may include existing gTLDs and all two-letter combinations to prevent confusion with the ISO 3166 list of country codes. Names with hyphens in the third and fourth positions are sometimes reserved until the registry is prepared to support Internationalised Domain Names (IDNs). This prevents bad faith or speculative registrations of ASCII-encoded mappings of names in non-Latin alphabets as well as the use of non-standard encodings of names in these scripts. Other reserved names can be found in a list published by ICANN. Its current schedule of reserved names is shown in Annex D. This list includes names like `dns`, `iana`, `ietf`, `nic` and acronyms for various components of the ICANN organisation and wider Internet community.

Although there is no requirement for an Administration to apply these conventions and withhold all or just some of these names, it would be prudent to do so. It should be noted that in many TLDs, names on ICANN's reserved list have already been registered. This is either because the registrations were made before the existence of ICANN or the TLD registry has not entered into an agreement with ICANN to reserve those names.

7.3.2 Nationally Sensitive Names

It may also be advisable for an Administration to add other names to a reserved list. These could take account of local cultural, religious, language and political factors as well as other expressions or names that are likely to cause offence or embarrassment. The choice of these nationally or culturally sensitive names will be a matter for the registry and the Administration alone. Wide consultation on the contents of such a list is recommended.

As a rule, it is very difficult to compile an effective list of offensive names. Registrants and registrars will find always imaginative ways to bypass such lists if the perceived value of the forbidden name is high enough. Updating and policing such lists can be an open-ended and very expensive resource drain. It is also possible for these lists to generate too many false positives: rejecting inoffensive names because they contain substrings that may be on a list of “naughty” words. For example AOL’s mail filtering software once blocked all messages that mentioned a large town in England because a substring in the town’s name was considered to be an indecent word. It also blocked any messages containing the word “breast” even when it was being used in email by medical professionals and support groups for cancer victims. These sorts of unintended effects can expose the registry to ridicule and bad publicity as well as litigation.

In other cases, the registration of a name might be conditional on the context in which it gets used. That can be very hard to establish at the time when the registration request is made. For instance a rule which banned the use of domain names containing the string “sex” would have some impact on the registration of names for pornographic or other obscene purposes. However it could also prevent a name such as `safesex.`*`ccTLD`* being registered to provide advice on protection against HIV and other sexually transmitted diseases. It will be necessary to strike a balance here and this may not be practical with a rule-based approach that does not involve some element of human judgement and common sense.

A pragmatic approach may be to compile a list of obviously inappropriate words or phrases and place these on a reserved list. A number of readily available mail filtering tools can provide some guidance on which terms should be on such a list. Names that are not on this list would be permitted to be registration subject to the registry’s standard terms and conditions. These could include a provision that domain names are not used for offensive, immoral or other harmful purposes. If the registrant does use the name for purposes that are unacceptable, they would be in breach of their registration agreement and sanctions could be taken against them. These could include cancellation of the domain name’s registration or, in extreme cases, civil or criminal proceedings. Patterns of sustained systematic abuse by a registrar could lead to the termination or suspension of their registry-registrar agreement and/or loss of accreditation. Obviously, there would be an escalation process before such steps were taken. There would presumably be some sort of independent adjudication panel that would act on complaints whenever a domain name was being used in ways that violated national or registry policy.

7.3.3 Premium and Novelty Names

Some new TLD registries have compiled lists of so-called premium names. These are names that may be held back from Sunrise and Landrush as well as at General Availability. The registry then makes these names available through some sort of auction. The name is then acquired and registered by the highest bidder.

The `.mobi` TLD has made the most extensive use of auctions of premium names to date. Results have been mixed. Overall the auctions have not raised as much as had been hoped. This may be partially due to the way in which the auctions were conducted and promoted. Some names failed to attract a buyer or proved to be less valuable than had been expected. Others raised remarkable fees: `flowers.mobi` was auctioned for $200,000. In 2006, the domain name `cameras.com` was sold for $1,500,000 though this did not involve a registry-operated auction. Detailed information about of the `.mobi` registry’s current reserved lists of premium and geographic names can be found at http://mtld.mobi/domain/premium and http://mtld.mobi/domain/reserved respectively.

A few ccTLDs have names that could attract unexpected registrations. The governments of Tuvalu and Turkmenistan make substantial amounts of money from registration of `.tv` (television) and `.tm` (trade mark) domain names respectively. These registrations have no association with the actual countries beyond the exploitation of their ccTLD names. If the ISO two-letter country code has these attributes, it would be worthwhile to compile a list of novelty names for a future auction and set these aside from any Landrush or General Availability sales.

Consideration should be given to the creation of a list of premium or novelty names and a process for raising extra income from their sale. It would probably be necessary to enter a partnership with a registrar or consultant specialising in premium names and their auction.

7.4 General Availability

The final stage of a TLD launch is General Availability, GA. At this point registration requests can be made by members of the public. Subject to the provisions of reserved names and eligibility criteria, requests would usually be handled on a first-come, first-served basis. Some parts of the name space may be set aside for particular communities rather than the general public. Even so, any member of a particular community would in principle by able to register a domain name. For instance, registrations in `com.ccTLD` might be restricted to locally-based businesses but any local company would be able to register a domain name under `com.ccTLD`.

The registry should have a complete set of policies in place by the start of General Availability. These will probably need to be incorporated into the registry’s terms and conditions: the contracts that it has with registrars and registrants. A mechanism for handling disputes will also be required.

7.5 On-Going Activities

Once the registry is up and running, it will enter a maintenance mode of operations. There will be a need for continuing outreach, customer support and training. The registry should develop and implement an outreach programme which explains to the local Internet community and general public how the registry operates and how its policy making is done. Customer support will also be required: helping registrants and registrars with any technical problems with their registration requests.

Registry staff should get involved in industry meetings and policy fora such as ICANN and IETF meetings so that they can at the very least track policy and protocol developments, especially those which might have public policy implications. They may even participate in these initiatives. The registry should also become a member of relevant trade associations such as AFTLD, the African Top-Level Domain Organisation, or CENTR, its European equivalent. This would allow registry management and technical staff to interact with their peers and get involved in regional and international aspects of the domain name business. The registry should also provide training and mentoring opportunities for its staff. AFTLD and AFRINIC, the African Regional Internet Registry, both hold regular workshops and training events which would be very appropriate for members of African ccTLD registries.

8 SUGGESTED PLAN

The first decision for an Administration is the choice of Sponsoring Organisation. If the *status quo* is not acceptable, the Administration needs to decide which entity should be responsible for the ccTLD. This would most likely be a government department or regulatory authority. Making that decision is a national matter and may well require consultation both within government circles and with the local Internet community as well as the general public.

It should be clear that once an Administration gets control of its ccTLD, there are many more things that need to be decided and a great deal of work remains to be done. Policies and procedures should be developed and these should fit with the Administration's wider public policy goals for Internet usage.

The most immediate concern is the nature of the ccTLD registry and its governance model. This will be the foundation for every other aspect of how the registry is operated and its policies are decided. Draft registry policies are easily obtained. Most registries publish these. However deciding which registry policies are appropriate for the ccTLD will depend on how the registry is to be structured and governed. Once those draft policies are prepared, some form of consultation and formal government approval will probably be needed. That may require a government process to be in place or these policies could simply be endorsed by the appropriate Minister in the Government. Registry policies that will be needed include: eligibility criteria, dispute resolution, whois, privacy, naming standards and possibly Sunrise and Landrush (if appropriate). Contracts and codes of conduct will also be needed: terms and conditions for registrants, a registry-registrar contract and perhaps some form of agreement with ICANN.

Parallel with the development of registry policies, potential staff for the registry should be identified and appointed. A suitably qualified chief executive is critical. He or she could take responsibility for the registry's initial policy development and the production of the registry's business plan. This business plan would indicate how the registry is expected to grow during its initial years, suggest how many staff are needed and what skills they would have, budgets, revenue and expenditure projections and so on. Another important part of the business plan will be to produce a time-line for the process that will advance the ccTLD towards an organisation that serves its community and meets the Administration's public policy objectives.

Technical decisions will also need to be taken by the registry. These will include where the registry is to be located (or when it should be moved) and what engineering staff and infrastructure will be needed. Performance criteria should be documented and care should be taken over the placement of the ccTLD's name servers. Guidance will be needed on the architecture of the systems needed for the registry as well as the protocols and interfaces it should support. Training for the registry's technical staff will probably be needed and it may be possible to arrange for the registry's staff to be mentored at other ccTLD or gTLD registries.

Finally it may be advisable to develop a launch plan for the ccTLD that takes account of the potential for Sunrise and Landrush phases that happen when new gTLDs are created.

9 ANNEX A – IANA GUIDE ON CCTLD DELEGATION AND RE-DELEGATION PROCEDURE

The text of this Annex can be found at http://www.iana.org/domains/root/delegation-guide/.

10 ANNEX B –BEST PRACTICE GUIDELINES FOR CCTLD REGISTRIES

The text of this Annex which is derived from related materials in the *ITU Handbook on Internet Protocol (IP)-Based Networks and Related Topics and Issues* (2005) available in Arabic, Chinese, English, French, Russian and Spanish on the ITU Development Sector's ICT Applications and Cybersecurity website[3] (Chapter 4.3.2) can be found at:

- Information on national practices for certain countries at: http://www.itu.int/ITU-T/special-projects/ip-policy/final/Attach10.doc
- Websites of particular ccTLDs accessed from http://www.iana.org/cctld/cctld-whois.htm
- ITU-T Workshop on Member States' experiences with ccTLDs, at http://www.itu.int/ITU-T/worksem/cctld/index.html
- TSB Circular 160, Addendum 2, which summarizes responses to a questionnaire on Member States' experiences with ccTLDs
- The best practices developed by a forum of ccTLD operators can be found at: http://www.itu.int/ITU-T/special-projects/ip-policy/final/Attach11.doc
- One particular generic ccTLD model can be found at: http://www.itu.int/ITU-T/special-projects/ip-policy/final/Attach12.doc

[3] http://www.itu.int/ITU-D/cyb/ip/

11 ANNEX C – COUNTRY CODE TOP-LEVEL DOMAIN BEST CURRENT PRACTICES

The text of this Annex can be found at http://www.nsrc.org/netadmin/cctld-bcp.html.

12 ANNEX D – ICANN SCHEDULE OF RESERVED NAMES

The text of this Annex can be found at http://www.icann.org/tlds/agreements/unsponsored/registry-agmt-appk-26apr01.htm.

13 ANNEX E – SAMPLE REGISTRY-REGISTRAR AGREEMENT

Samples registry-registrar agreeements can be found at http://www.icann.org/registries/agreements.htm.