A Study Proposal for Examining the User Experience Implications of Active Variant TLDs

Preliminary Discussion Draft

20-Jun-2012

Table of Contents

1. Motivation for the Project[1]

Should the Internet Corporation of Assigned Names and Numbers (ICANN) activate variant top-level domains (TLD) in the root, many parts of the Internet ecosystem will be affected, with corresponding impacts on the user experience. Examples of user roles that have been identified previously include registrants, registrars, registry operators, system administrators, network operators, application developers, and end users. As the coordination body for the Domain Name System (DNS), ICANN has a responsibility to investigate possible impacts of new developments, and to proactively identify and publicize potential issues. Implementation of variant TLDs without adequate consideration of outcomes such as user confusion, inconsistent and error-prone experience, or security risks could lead to significant gaps in the desired results.

The study will consider the user roles identified in the Integrated Issues Report (ICANN, 2011), and the impacts to these users should variant TLDs be activated. Based on the study findings, a definition for a good user experience can be specified and subsequently used as a means for discussing, considering, and assessing performance. Based on the factors identified in the study, additional steps may be recommended to support a good user experience with regard to variant TLDs. To the best of our knowledge, no systematic study has been done in this area, therefore the proposed work fills this gap.

Registry and registrar policies will most likely play an important role in shaping the user experience with variant TLDs. Given the need for a cautious approach in the early stages, these operators may be subject to a more stringent set of requirements to minimize the possibility of user confusion, inconsistent user experience, security risks or long-term Internet instability. In this regard, the study will identify a set of factors for acceptable user experiences, some of which could be mapped onto requirements to be written into contracts where possible, others could be turned into best practices or guidelines for the various domain name stakeholders.

It should be noted that ICANN has no direct control or influence over many issues that the study may identify. For example: system administrators' need for automated tools to configure web and email servers or applications not able to handle variants. In these areas, it is still helpful to raise and communicate these issues to the relevant affected communities. This could also help the communities interested in the implementation of variant TLDs to focus their efforts in improving the user experience.

Last but not least, the root is a special shared resource by all user communities. Policies and best practices set at the root level should be fair, consistent and conservative. Such policies couldinfluence TLD and SLD policies. This study will contribute to this overall policy goal.

[1] As given in *IDN Variant TLD Program - Revised Program Plan* available at http://www.icann.org/en/news/public-comment/idn-variant-tld-revised-program-plan-04may12-en.htm

2. General Notes

The terminology used in this document follows the conventions being recommended by the community and as documented/defined by ICANN (2011),particularly in "Appendix 2: Terminology". Readers should understand these definitions of relevant terms given, especially those for *Variant Label, Label Generation Rules, Fundamental Label, IDL Set, U-Label, A-Label* and other terms used in this document.

Given that the Label Generation Rules for creating a variant label are not yet defined, the document will use *example.TLDv1, example.TLDv2, …, example.TLDvN* to indicate *N* variant labels of the top level domain TLD in this document. The corresponding zone files may not be identical or mirrored.

There are ongoing discussions on how variant labels will be implemented. Though much of the document may remain relevant irrespective of the method used to implement variants, the final implementation could still have impact on this study, while possibly introducing additional issues not discussed in this document.

ICANN (2011), based on discussion in various case study teams (for Arabic, Chinese, Cyrillic, Devanagari, Greek and Latin), identifies multiple states and transitions possible for variant labels in Section 5 of their report, "Discussion of Issues: Treatment of Variant Labels". This life cycle for variants has to be finalized by the community, and the decisions eventually taken may also have impact on the findings of this report, because once the states have been defined, all stake holders will need to understand the states and transition process between the and then enable processes to manage them.

3. Scope of Work

As defined by *IDN Variant TLD Program - Revised Program Plan*[1], the current study is intended to investigate the following questions:

- What are the components of an acceptable user experience for variant TLDs?
- What are the necessary rules or guidelines a TLD should operate under in order to provide an acceptable user experience for variants?
- What are the policy/contractual considerations that will make these rules effective?
- How does the impact of variant TLDs on applications affect user experience?
- What other entities have a critical role to play in addressing these issues and what educational or consultative steps could be implemented to generate support and collaboration by these parties?

Based on the investigation, the study is intended to have the following outcomes:

1. Recommended rules or guidelines for various stakeholders to provide an acceptable user experience with regard to variant TLDs, including appropriate policy or contractual provisions to make these rules effective.

2. Creation of a useful reference for educating application developers and others affected by

these changes.

4. Background and Related Work

4.1. Usability and User Experience

The International Standards Organization in its standard IS0 9241-11:1998(E) (ISO, 1998) defines usability as:

> the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.

Usability has multiple components and is traditionally associated with these five attributes (Nielsen, 1993):

- Learnability: the system should be easy to learn so that the user can rapidly start getting some work done with the system.
- Efficiency: The system should be efficient to use so that once the user has learned the system, a high level of productivity is possible.
- Memorability: The system should be easy to remember so that the casual user is able to return to the system after some period of not having used it without having to learn everything all over again.
- Error tolerance and prevention: The system should have a low error rate so that users make few errors during the use of the system, and so that if they do make error they can recover from them. Further catastrophic errors must not occur.
- Satisfaction: The system should be pleasant to use so that users are subjectively satisfied when using it; they like it.

Some people distinguish between usability and user experience. Usability is usually considered the ability of the user to use the system to carry out a task successfully, whereas user experience takes a broader view, looking at the individual's entire interaction with the system, as well as the thoughts, feelings and perceptions that result from the interaction (Tullia and Albert, 2008).

In this report, we took a narrower view in terms of user experience by focusing just on the usability aspect.

4.2. System Acceptability

System acceptability (Nielsen, 1993) concerns the question of whether the system is good enough to satisfy all the needs and requirements of the system users and other potential stakeholders. Figure 1 shows the simple model of system acceptability. It contains several components that are explained below.

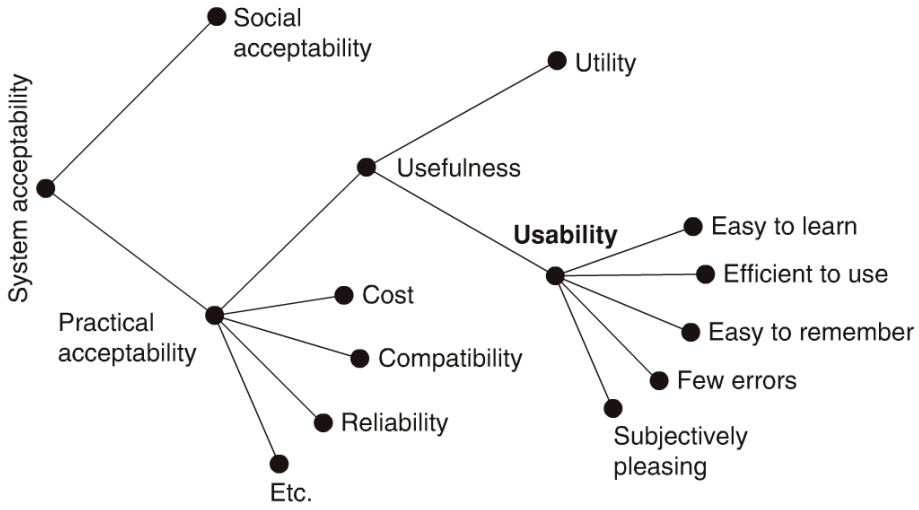


Figure 1: A model of the attributes of system acceptability (Nielson, 1993)

The overall acceptability of a system is a combination of social acceptability and its practical acceptability. Social acceptability concerns whether a system is socially desirable, meets the needs of particular groups of users while balancing the concerns of other users.

Given that a system is socially acceptable, one can further analyze its practical acceptability within various categories, including traditional categories such as cost, support, reliability, compatibility with existing systems, as well as the category of usefulness. Usefulness is the issue of whether the system can be used to achieve some desired goal. It can be further broken down into two categories, utility and usability (Grudin, 1992), where utility is the question of whether the functionality of the system is what is needed and usability is the question of how well users can use that functionality.

It is important to note that some of the issues are related to variants only, and are not a problem for general IDNs, while other problems are related to IDNs directly. This report will distinguish the two, and focus specifically on IDN variants issues, and not general IDN issues.

Finally it is worth noting that IDNs are just beginning to get adopted, and there will be many issues towards acceptance as the usage increases. For example, until recently the SMTP protocol could not handle internationalized email addresses, and many other protocols have still not been internationalized. The issues of technical acceptance, user experience and user demand are interrelated. So the community needs to balance the user demand and the potential limitations and risks in a pragmatic way as it discusses the implementation of variants going forward.

4.3. Related Work (this section under development)

In this section, we highlight some related work in this area.

Universal Acceptance of all TLDs project: http://www.icann.org/en/resources/tld-acceptance

RFC 3696: Application Techniques for Checking and Transformation of Names

Work on Domain Name Registration Data – SSAC, IETF, WHOIS Review Team, …

5. Proposed Methodology

The study intends to identify various user roles, how these users may be impacted by introducing variant TLDs, and what may be done to address any issues identified.

5.1. Identify User Roles

Domain names, which may be registered as variant TLDs, are used in a variety of contexts by a variety of users. Identifying this variety of user roles for this study is a key task and the necessary first step to undertake such a study. The starting point for determining the user roles has been the review of the six individual case studies by the Arabic, Chinese, Cyrillic, Devanagari, Greek and Latin script communities for the IDN Variant Issues Project and the subsequent Integrated Issues Report. While the current study team has also been brainstorming additional roles to ensure maximal coverage, the study team will solicit the feedback from the community to identify additional potentially relevant actors.

At this time the team is taking a liberal approach and including all the potentially relevant actors. The relevant actors will be short-listed from this larger set in the analysis phase of the project.

5.2. Identify Potential Use Cases for each User Role

As the potentially relevant user roles are identified, the next step is to identify how they interact with the system(s) using domain names. These relevant uses need to be further studied to ascertain any specific impact of TLD variants. The study team has currently been identifying the variety of ways a user may use a domain name to study the potential impact of the variant TLDs. Further feedback will be requested from the community to (i) comment on the uses already identified, and (ii) suggest additional uses which may be impacted by variant TLDs.

5.3. Analyze the Impact of Variant TLDs

As the identification of user roles and potential relevant use cases of the system(s) are finalized through the study and community feedback (through public comment), the project team will start the analysis of each of the use cases to determine the impact of variant TLDs. If the use case is found relevant, the issue will be further studied. The analysis will address multiple aspects, including usability, technology, contracts, compliance, policy and training.

The analysis phase will include different methods for different user roles, including interviews and online surveys. The team may also consider usability experiments in certain cases. These are summarized in Section 7 later.

The analysis done and draft recommendations will be submitted for public consultation from the community for further feedback. These will also be presented in a public session at ICANN meeting in Toronto (if possible) for more extensive discussions.

5.4. Finalizing the Analysis and Recommendations

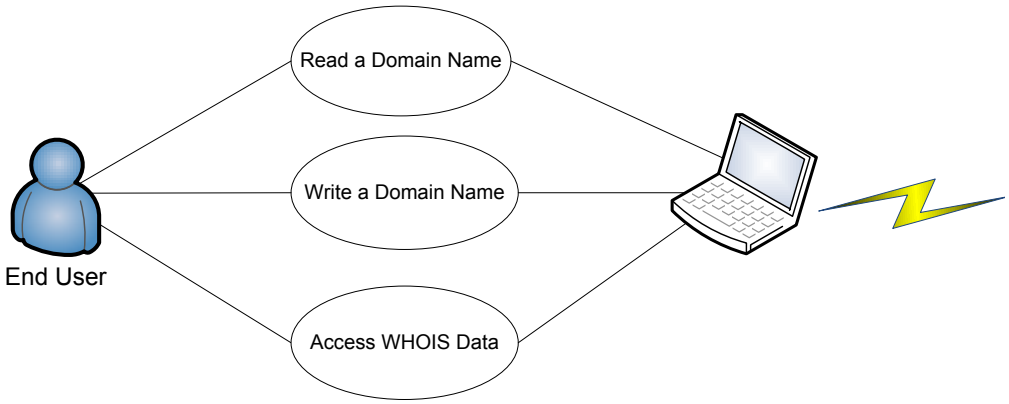
In the final phase, the public consultation on the analysis will be incorporated and the recommendations and next steps will be finalized.

6. User Roles and Use Cases

There are many different users interacting with systems and using domain names in different contexts. This sections attempts to list the most visible users and identify some significant ways in which these users may use a domain name.

6.1. End User

End users use the Internet for a variety of commonly understood functions. These include web browsing, email, desktop publishing, file transfers, etc. They access these functions using a variety of devices, user input/output methods software system configurations, software applications, and networks. This variety makes this user role very challenging to assess. However, even though the user undertakes a variety of tasks, they can be categorized in two logical tasks in the context of domain names: (i) read a domain name, and (ii) write/type/enter a domain name. In addition, the end user may also access WHOIS related data for a given domain name through various services.



The following is a non-exhaustive list of contexts in which these use cases may be performed by an End User. In addition, other specific use cases are also identified:

1. Read a domain name
   1.1. In a variety of languages and scripts (e.g. a script level variant considered by a language community as a distinct label)

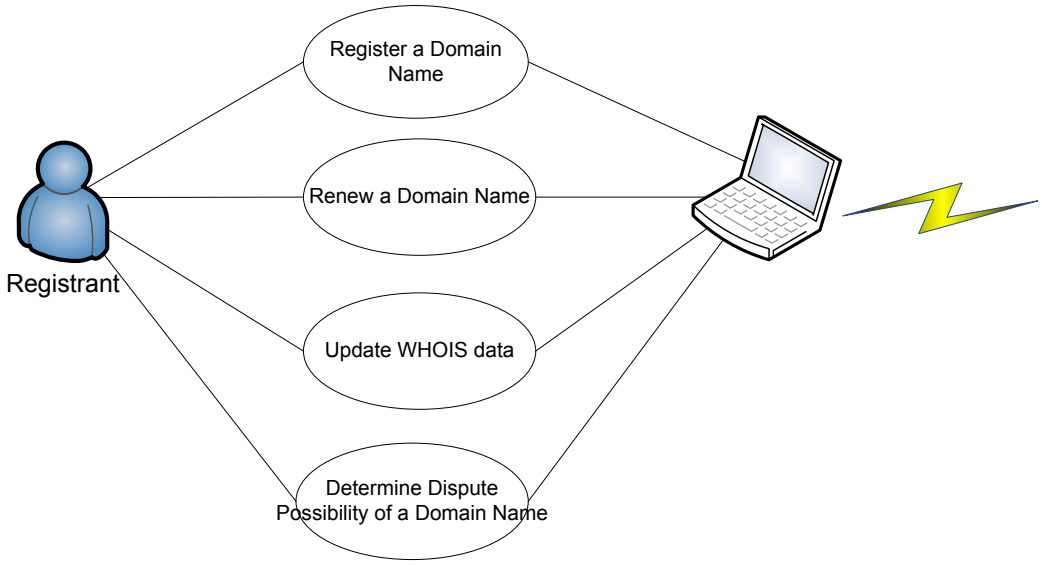
1.2. With encoding challenges (bidi, non-Alphabetic characters)
1.3. Understand difference in A-Label for "same" U-Label (for systems which display A-Label)?
1.4. Using a variety of fonts
1.5. In a variety of applications
1.6. Using a variety of locale configurations
1.7. Using a variety of Operating Systems
1.8. Using a variety of other modalities (published material, advertisements, etc.)

2. Write a domain name
   2.1. In a variety of languages and scripts (e.g. a script level variant considered by a language community as a distinct label)
   2.2. With encoding challenges (bidi, non-Alphabetic characters)
   2.3. In a variety of applications (web browser, email client, chat client, etc.)
   2.4. Using a variety of locale configurations
   2.5. Using a variety of Operating Systems
   2.6. Using a variety of devices (computers, mobile phones)
   2.7. Using a variety of input devices (keyboard, onscreen keyboard, Mobile Keypad, Voice)
   2.8. Using a variety of input methods[2]
   2.9. Using other methods (than inputting characters) such as copy/paste, auto-complete, etc.
3. Access WHOIS data for a domain through various user interfaces and query methods (web, WHOIS protocol, WHOIS third-party services, etc.)
   3.1. Understanding WHOIS data representation scheme for Internationalized Domain Label (IDL) set
   3.2. Accessing WHOIS data for IDL set
   3.3. Reporting rendering issues of WHOIS service for a variant TLD to registrars, registries and/or ICANN[3]

6.2. Registrant

Registrants would interact with the DNS through the registrar interface, to register or renew a domain name. In addition, the registrant would also update its WHOIS entry and check for confusability of a domain name against disputes, both to do preventive registration (to protect a trademark, etc. or for mal-intentions, e.g. cyber squatting).

[2] For example see http://en.wikipedia.org/wiki/Chinese_input_methods_for_computers for Chinese script
[3] For ICANN, see Whois Data Problem Reporting System (WDPRS)



1. Register a Domain Name
   1.1. Understanding how a label is a variant of another label and its relevant implications
   1.2. Reporting rendering/display issue for a variant label
   1.3. Choosing a Fundamental Label (if given a choice)
   1.4. Choosing which labels to activate (if given a choice)
   1.5. Understanding differing pricing models for (across registrars) registration of a variant
   1.6. Changing an active IDL set (changing Fundamental Label? Activating an inactive label? De-activating an active label?)
   1.7. Understanding pricing model for (across registrars) changing an IDL set
   1.8. Binding the variants and their relevant domain services
   1.9. End-user writing a domain name (see relevant section) in the registration process
   1.10. Understanding errors and issues of unacceptable variants sent by the registrar
2. Renew a Domain Name
   2.1. Renewing an existing domain name, adding variant TLDs (assuming the latter are introduced after the existing domain name is registered)
   2.2. Renewing a IDL set (all possibilities; see *Register a Domain Name*)
3. Update a WHOIS entry associated with a domain name
   3.1. Creating WHOIS entry for a Fundamental Label? IDL set? Different WHOIS data for variants, e.g. starting and ending dates?
   3.2. Reporting rendering issues in a WHOIS entry
   3.3. Updating WHOIS entry at renewal?
   3.4. Updating WHOIS entry for change in IDL set?
   3.5. Adding WHOIS information against a domain name which was registered before the introduction of variant TLDs
4. Determine the possibility of dispute of variants of domain being registered

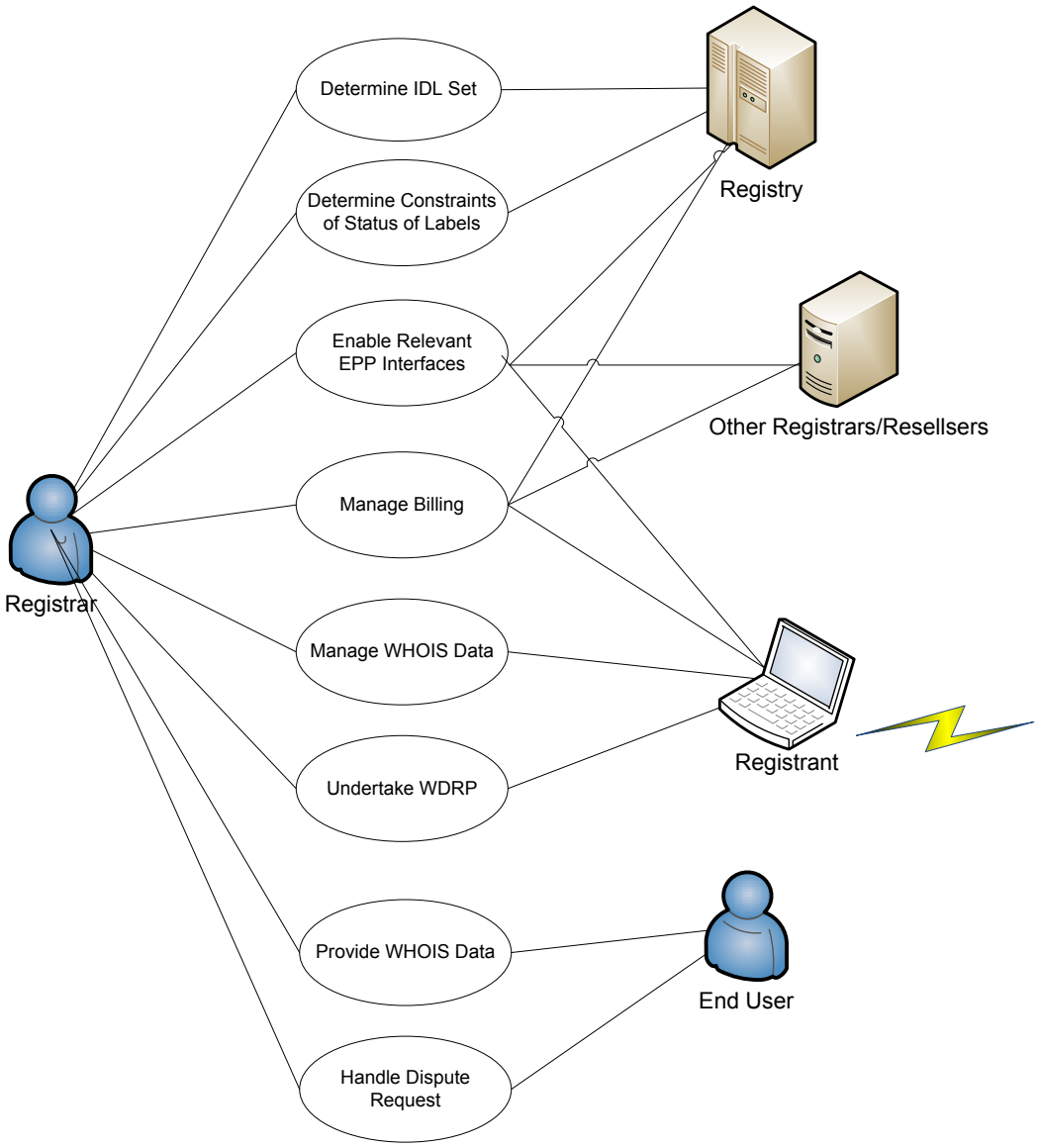
6.3. Resellers, Proxy and Privacy Services

Resellers, privacy and proxy services are roles identified in the RAA[4]. These services act on behalf of the registrant and may perform many of the functions on behalf of the registrant with the registrar. They also escrow data of the registrants. They may have specific functions, in addition to the functions available to registrants. These services may have similar impacts as identified in the section on Registrars. These functions are not governed directly by ICANN, but through sub-contracts with registrars. The study should also identify any unique functions, and how to best enable them for variant TLDs.

6.4. Registrar

Registrar provides interfaces to a variety of clients, including end-users, registrants, registrars, proxy/privacy providers, re-sellers and ICANN. Use cases relevant to registrars who may be impacted due to introduction of variant TLDs are given below.

[4] Available at http://www.icann.org/en/resources/registrars/raa/ra-agreement-21may09-en.htm



1. Generate IDL set against a label using the Label Generation Rules (undefined at this time)
2. Check what possible statuses various members of IDL set may take
3. Check Domain action in EPP: (this can take more than one domain so may work as it is, but is there need to distinguish between variants and other domains?)
4. Create Domain action in EPP: (this can take more than one domain so may work as it is, but is there need to distinguish between variants and other domains?) Other complications include: (i) status of variant, (ii) time for each variant (same or can be different?), (iii) nameservers, (iv) contact information, if it is possible to have different contacts for different variants, etc.
5. Get Domain Info in EPP
6. Update action in EPP (domain, contacts, host; how to tie this with variants?)
7. Delete action in EPP (implications on deleting a variant with a particular status; what if fundamental domain name is deleted, what happens to the rest: another becomes fundamental? How? Or all associated variants deleted?)

8. Domain Renewal action in EPP – which one of the variant, all of them at the same time?
9. Domain Transfer action inEPP – what is variant policies are different across registrars, re. status, fundamental, pricing, etc.
10. Additional Response Codes for Variant management in EPP, and appropriate information (for the end-user) on why the variant has not been accepted
11. Manage billing with different clients/suppliers
12. Manage escrow service (what should be escrowed in an IDL set?)
13. Releasing first-time variants for registration against existing active domain names and managing conflicts caused by Label Generation Rules (designed at script level)
    a. gTLD (script level)
    b. ccTLD (potentially mono- or multi-lingual, but may not cover whole script)
14. For many actions, could variants be handled by different registrars? What happens if one variant is transferred/expired/renewed but not the others?
15. Handling multiple user identifiers, if variants could be registered to different user identifiers while being the same owner
16. Extend and manage WHOIS Data Reminders (WDRP) for variants? (http://www.icann.org/en/resources/registrars/consensus-policies/wdrp)
17. Handle dispute request from an end user, in the context of UDRP

6.5. Dispute Resolution Service Provider

Introducing variants may introduce new kinds of disputes and may require visiting the UDRP and/or the associated process. UDRP (http://www.icann.org/en/help/dndr/udrp/policy) Sections 4a and 4b are applicable to a domain name. How will this be applicable to an IDL set? e.g. determining "Bad Faith" of variant(s) (e.g., if they are automatically generated against a Fundamental Label, and if latter does not cause a direct conflict but some variant(s) do). Also, will this require re-certification of Approved Dispute Resolution Service Providers[5]? If yes, what will be the process of re-certification?

Would the variants also have implications on ccTLD dispute resolution practices and policies, which are governed by national laws – what if these conflict with Label Generation Rules at ICANN – how will such cases be resolved? Should the Label Generation Rules, which are to be defined with the help of the community, have input from GAC to address such future issues?

If there are implications, relevant contracts, policies and compliance measures need to be appropriately updated. These will need to be identified.

6.6. Registry

Registry interfaces with many different users providing a variety of services. It provides EPP interface to Registrars, hosts DNS Server, WHOIS server, maintains performance and security

[5] List available at http://www.icann.org/en/help/dndr/udrp/providers

analytics, and interfaces with ICANN for payments and performance. Introduction of variants at TLD level may have impact on one of more of the following functions it performs.

1. Managing the TLD using various tools
2. Enabling appropriate EPP Interfaces with Registrars (see the section on Registrars for further details)
3. Hosting and maintaining a DNS Server, including maintaining the Zone file(s))
4. Hosting and maintaining a WHOIS Server
5. Managing billing with registrars
6. Measuring relevant system analytics –
7. Deploying and maintaining security software
8. Managing data escrow
9. Developing a pricing policy (payments to ICANN based on fundamental or all variants)
10. Monthly reporting to ICANN
11. Managing sunrise and trademark claims processes using variants for new registries
12. Releasing first-time variants for registration against existing active domain names and managing conflicts caused by Label Generation Rules (designed at script level)
    a. gTLD (script level)
    b. ccTLD (potentially mono- or multi-lingual, but may not cover whole script)

6.7. ICANN

1. As root server operator, manage variant TLDs.
2. Compliance Function
   2.1. WHOIS data accuracy
   2.2. WHOIS data reminder policy
   2.3. Consensus policies
3. As manager of the various registries, manage variant TLDs (IANA function)

6.8. System Administrators

In many organizations, the boundary of system, network and security administrators may not be well defined. For the purpose of this study, we define the three roles with the minimum overlap.

For the purpose of this study (intended that this task list is shorter than reality), a system administrator accomplishes at least the following tasks: configuring and provisioning computers, OS, services, and monitoring services; performance management; management of user accounts and identifiers; and management of certificates.

1. The system administrator writes hostnames and domain names in various configuration panels and files to perform these tasks
2. For monitoring and performance management, search and match hostnames and domain names against various logging facilities using U-labels and A-labels
3. Most common system administration tools have not been updated to fully support IDNs. In this context, the system administrator has to configure, search, match and manage A-labels for

hostnames and domain names. Thus, system administrator may also have to match and bind two (or more) labels in an IDL set visible as different A-labels

4. Implement the equivalence (or non-equivalence depending on the desired end-result) of variants in the configuration of servers and services.
    a. Some system tools are ready to manage multiple hostnames or domain names, either with multiple independent sets of configuration objects or with aliases.

        When multiple independent sets of configuration objects are used, then it is up to the system administrator to correctly replicate the configuration data for each variant. Failure to duplicate will create errors or different behaviors. For example, virtual hosting for the Apache server is made this way.

        Aliasing is usually less error or data duplication issues prone, since the service is making the two hostnames or domain names equivalent. However, there is usually a primary name and aliases. The primary name is often used for logging and other configuration data, therefore, the aliases may not be seen and processed equally in the system. For example, configuration of network interfaces and hosts tables on Linux are made this way.

    In both cases, the variant is not fully equivalent in the tools and therefore is prone to errors or misbehaviors.

    b. Some system tools or services are not ready to manage multiple hostnames or domain names, either because the tool has no concept of multiple equivalent hostnames or because equivalent names are against the service policy.

        For example, TLS is used by web servers to secure the communication between the client and the server. TLS requires a certificate containing the hostname of the server and the public key. If two hostnames are equivalent as for variants, then two certificates are to be issued, configured and managed completely separately.

        Similarly, if the variants are managed using different DNS zone files, then the DNSSEC signatures are to be issued, configured and managed separately.

6.9. Network Managers

For the purpose of this study, a network manager accomplishes the following tasks: configuring and provisioning routers, switches and network applications; monitoring network resources; and managing performance.

1. Implement the equivalence (or non-equivalence depending on the desired end-result) of variants in the configuration of network resources

Network object configuration may contain domain names or hostnames. In many cases, these are not critical to the function of the network object. In most cases, there are very limited capabilities of aliases or fully equivalent names. Therefore, the variants are often not possible to be entered into network object configurations. For example, a router hostname is often a single hostname configuration line.

2. Network administrators are often performing monitoring and performance management using various logging facilities.

   These logging records come from various network objects for events happening in the network. Given that these objects are not handling variants, the aggregation of logging records will not make any search or match for variants either.

6.10. Security Administrator/Law Enforcement Agency

For the purpose of this study, a security administrator accomplishes the following tasks: configuring and provisioning firewalls, VPNs and security policies on various network resources and servers; and monitoring security and logs.

1. Implement the equivalence (or non-equivalence depending on the desired end-result) of variants in the configuration of security policies. Security policies are configured using various data sets, sometimes with hostnames or domain names. As these systems do not have the notion of variants (on purpose or not), the duplication of policies for each variant may be needed.

2. Match variants in logging. When a security event happens, logging records are looked and an investigation is made. If the logging records are not fully bound together with variants, then the investigation may lead to a false or incorrect result.

3. Forensics and identify subjects for investigation

   Tracking variants may also become more difficult based on how the WHOIS records of variants are maintained. Variants in additions to IDNs will compound the issues of tracking them.

   Tracking variants may become even more cumbersome or difficult if the variants can change state (e.g. de-activated, which may make its WHOIS record unavailable).

4. Filter Spam: One of the techniques to filter spam and other filter applications is by maintaining a list of domain names, in addition to rules, which are applied to the traffic passing through the network. If a domain name is added or removed from such a list, all of its variants should also be appropriately handled.

6.11. Application Developers

Application developers need to make applications aware of variants, where relevant, for a variety of users.

1. Some applications maintain a list of TLDs to enable U-Label display instead of A-Label[6]. Variants need to be taken into account.
2. When TLDs are used to verify the existence of a domain name, these functions shall be updated for variants. For example, some web browser implementers maintain a common list of TLDs [ref: http://publicsuffixes.org) to manage auto-completion and other end-user services.
3. Software has smarts to identify domain names and URLs within their interface, user input or documents. What to do with variants?
4. Software offers to end-users various search mechanisms. What to do with variants?
5. Software access network resources using various OS API, which uses domain names and URLs. What to do with variants?
6. Software do domain name matching and searching. What to do with variants?

7. Tentative Work Plan and Timelines

The tentative work plan for collection and analysis of data is given is summarized below. The work will include getting feedback through a survey and/or group discussions with relevant user communities. It is anticipated that there will be face-to-face discussion opportunities with many of the groups at ICANN Prague meeting, especially with registrars, gTLDs, ccTLDs, Compliance Team at ICANN, and Law Enforcement Agencies (LEAs). For organizing feedback from Application Developers, Network Managers and Security Administrators, attending next IETF meeting in Vancouver, Canada is being considered.

For those with whom face to face interaction is not easily possible, surveys will be developed and circulated online for gathering relevant data. Multiple surveys will be designed for various stakeholders, as per the details in the table below.

In addition to the surveys and group discussions, interviews will also be organized with some communities for more detailed discussions through teleconferencing. In a few cases, site visits are also being considered. These are especially relevant for ccTLDs who already have experience with IDNs and are considering (or already implementing) variants. These specifically include Chinese and Arabic scripts. Visits to registrars for more detailed operational and technical analysis are also being considered, as registrars will be one of the most affected users due to the introduction to variant TLDs.

In addition, for the wider end user community, which specifically requires extensive training but does not come directly under the ambit of ICANN, some end user experiments may also be designed to get further intuition into their behavior in the context of the challenge IDN variants may pose.

[6] For example, see the IDN TLD list maintained by Mozilla at http://www.mozilla.org/projects/security/tld-idn-policy-list.html.

Finally, all the work being done will be released for public consultation and feedback at various stages (as already discussed in the Section on Methodology).This is summarized in the table below.

Table 1: A Summary of the Proposed Work

Method / User	Survey/ Focus Group	Interview	Visit	Usability Experiments (if possible)	Public Consultation
End User	x (survey)			x	x
Registrant	x (survey)				x
Resellers/Proxy/ Privacy	x (ICANN meeting)	x			x
Registrar	x (ICANN meeting)		x		x
Dispute Resolution Service Provider		x			x
Registry (gTLD, ccTLD)	x (ICANN meeting)		x (ccTLDs using IDNs, e.g. for Chinese and Arabic script)		x
ICANN (compliance team)	x (ICANN meeting)	x			x
System Administrator	x (IETF Meeting)			x	x
Network Manager	x (IETF Meeting)			x	x
Security Administrator/LEA	x (IETF/ICANN Meeting)	x			x
Application Developers	x (survey)				x

The project has started in late May 2012. The team has worked over past month to develop the current document in time for public consultation at ICANN meeting being held in Prague in June 2012. After feedback from the community, the project team will implement the proposed study and produce a draft report by September 2012. The draft report will be released for public comment in September and presented for public consultation at ICANN meeting in Toronto in October 2012. Based on public feedback, the report will be finalized by December 2012 and released for final public feedback in January 2013. The team will finalize the report in early February 2013 and close the project.

8. First Public Consultation

The first public consultation for the project asks for general response from the community on all relevant aspects, and specifically on the following queries:

1. Are there any other significant user roles, beyond those identified?
2. Are there any use cases for the roles identified which may be relevant in the context of IDN variant TLDs, but have not been listed?
3. Are there any use cases for the roles identified which may not be relevant in the context of IDN variant TLDs, but have been listed?

References

Arabic Case Study Team (2011).*Internationalized Domain Names Variant Issues Project: Arabic Case Study Team Issues Report.* ICANN. Available at http://www.icann.org/en/resources/idn/variant-tlds.

Chinese Case Study Team (2011).*Report on Chinese Variants in Internationalized Top-Level*

Domains. ICANN. Available at http://www.icann.org/en/resources/idn/variant-tlds.

Cyrillic Case Study Team (2011).*IDN Variant TLDs – Cyrillic Script Issues.* ICANN. Available at http://www.icann.org/en/resources/idn/variant-tlds.

Devanagari Case Study Team (2011).*Devanāgarī VIP Team Issues Report.* ICANN. Available at http://www.icann.org/en/resources/idn/variant-tlds.

Greek Case Study Team (2011). *Study of the Issues Present in the Registration of IDN TLDs in Greek Characters.* ICANN. Available at http://www.icann.org/en/resources/idn/variant-tlds.

J. Grudin (1992). "Utility and Usability: Research Issues and Development Contexts," *Interacting with Computers*, 4(2): 209–217.

ICANN (2011).*A Study of Issues Related to the Management of IDN Variant TLDs (Integrated Issues Report).*ICANN. Available at http://www.icann.org/en/resources/idn/variant-tlds.

ISO (1998).*Ergonomic requirements for office work with visual display terminals (VDTs) - Part 11 : Guidance on usability*. ISO 9241-1998(E).International Standards Organization (ISO), Geneva, Switzerland.

Latin Case Study Team (2011).*Consideration in the Use of the Latin Script in the Variant Internationalized Top-Level Domain.* ICANN. Available at http://www.icann.org/en/resources/idn/variant-tlds.

J. Nielsen (1993). *Usability Engineering*. Morgan Kaufmann, San Francisco, CA, USA.

T. Tulllia, and W. Albert (2008). *Measuring the User Experience: Collecting, Analyzing, and Presenting Usability Metrics*, Morgan Kaufmann, San Francisco, USA.

Appendix A: DNS records and their variants impacts

This appendix discusses about the various DNS record types and their impacts on variants. While not exhaustive and not conformant, this list will help the various user roles discussions to understand the implications of variants depending on the DNS record type.

Address and PTR records: A PTR record maps an IP address to a name. Impacts when multiple equivalent names such as variants should be discussed.

CNAME record: A CNAME record creates an alternate name. Impacts when multiple equivalent names such as variants should be discussed.

MX record: A MX record identifies an ordered list of email servers ready to receive email for the domain. Impacts when multiple equivalent names such as variants should be discussed.

SRV records: SRV records identify servers responsible for services, using a powerful syntax. Impacts when multiple equivalent names such as variants should be discussed.

SPF records: SPF records are experimental but widely used TXT DNS records to identify which email servers the emails of a domain should be sent from. They are used for spam filtering. Impacts when multiple equivalent names such as variants should be discussed.