



IDN ccTLD Fast Track Program Proposed Implementation Details Regarding:

Documentation of Responsibility between ICANN and prospective IDN ccTLD managers

Date of Publication:

18 February 2009

Background – IDN ccTLD Fast Track Process

One of the most significant innovations in the Internet since its inception will be the introduction of top level Internationalized Domain Names (IDNs). These IDNs will offer many new opportunities and benefits for Internet users around the world by allowing them to establish and use domains in their native languages and scripts.

The topic of IDNs has been discussed in the ICANN community for a number of years. Initially, development was focused on enabling the introduction of IDNs as registrations under existing TLDs, but focus has shifted to be on broadening the characters repertoire available for use in top level strings as well. The IDN ccTLD Fast Track Process is one process ICANN is working on that will enable such introduction. The process for implementation of new gTLDs will also support Internationalized Top Level domains as part of the new [gTLD program](#).

The initial steps for introduction of IDN ccTLDs were initiated by the ICANN Board at its meeting in Sao Paulo (December 2006). During consultations and discussions of the then joint GAC and ccNSO IDN working group, it became clear that a number of countries and territories have a pressing need for IDN ccTLDs. The IDN ccTLD Fast Track Process is specifically aiming at meeting this near-term demand and at gaining experience with the mechanisms for selection and authorization of such TLDs that can inform the ongoing long-term policy development process.

The implementation of the IDN ccTLD Fast Track Process is underway and it based on the [Final Report](#) of the [IDNC Working Group](#), recommending mechanisms to introduce a limited number of non contentious IDN ccTLDs, associated with the ISO 3166-1 two-letter codes. In the [initial Draft Implementation Plan](#) for the IDN ccTLD fast Track Process a number of open issues were identified that require further input from the community and need to be resolved, to complete the implementation.

This paper is part of a series of papers that will serve as proposed solutions to these open issues. The proposed solutions are based on public comments and input received through meetings, such as those held during the ICANN meeting in Cairo, Egypt, November 3–7, 2008. The papers are being posted in conjunction with an updated Draft Implementation Plan to seek further community collaborations, in particular before and during the ICANN Meeting in Mexico City, Mexico, March 1–6, 2009. A public comment period for these papers will enable and document such community discussions. Received comments will then be used to revise the plan in preparation of a Final Implementation Plan.

Please note that this is a proposed discussion draft only. Potential IDN ccTLD requestors should not rely on any of the proposed included details as it remains subject to further consultation and revision.

A full overview of activities related to the IDN ccTLD Fast Track process and implementation thereof can be viewed at <http://www.icann.org/en/topics/idn/fast-track/>.

Draft—for discussion only—please refer to the disclaimer on the title page of this document.

Summary of Key Points in this Paper

- A formal arrangement between ICANN and potential IDN ccTLD managers is required to ensure security, stability and interoperability of the DNS. It is also important to ICANN's program of accountability and transparency. The proposed formal arrangement, referred to as a, "Documentation of Responsibilities (DoR), is based on the Accountability Framework program, with additional elements to ensure compliance with IDN related technical standards.
- Comments are sought on the proposed Documentation of Responsibilities.

Executive Summary

Discussion and Rationale for a formal arrangement between ICANN and IDN ccTLD managers

One topic introduced for further community discussion in [the initial implementation planning work](#) was the relationship between ICANN and the IDN ccTLD manager after delegation of the IDN ccTLD(s). The IDNC WG was silent on the specifics of this topic; however, the need and nature of such a relationship was considered extensively in the comments received on the IDNC WG Final Report.

The IDNC WG accepted and developed its recommendations within the following overarching requirements set by the ICANN Board:

- Preserve the security and stability of the DNS;
- Comply with the IDNA protocols and IDN guidelines;
- Take input and advice from the technical community with respect to the implementation of IDNs; and
- Comply with current practices for the delegation of ccTLDs, which include the current IANA practices, amongst others, RFC 1591 and the GAC ccTLD Principles.

Additionally, the IDNC WG developed guiding principles which, within the context of the overarching requirements, structure, guide and set conditions for the methodology for introducing IDN ccTLDs under the fast track process. One guiding principle that is important to consider in the context of the relationship between ICANN and the IDN ccTLD manager is the experimental nature¹ of the introduction of IDN ccTLDs. The IDNC WG noted:

"F: The Fast Track is experimental in nature"

¹ It is important to note that by "experimental," the working group was commenting on the policy aspects of IDN introduction and not the technical aspects. IDNs have been tested in the root zone and technical implications of the introduction are generally well understood. All studies will be completed to ensure there is a full understanding that IDNs will have no deleterious effects on DNS interoperability, stability and security.

The introduction of IDN ccTLDs is experimental in nature, and therefore should not be considered to be precedent setting. The experimental nature of the Fast Track should also be taken into consideration when delegating names under the Fast Track. However, this should not be interpreted to mean that a delegation under the Fast Track will be temporary."

This comment from the IDNC WG highlights the fact that IDNs are still in their earliest implementation phase, with the conclusion that adherence to relevant technical guidelines is important, particularly given that these new IDN TLDs will be delegated permanently.

The [draft Implementation Plan](#) (26 November 2008) contemplated a structure to the relationships between ICANN and the IDN ccTLD manager (i.e., that this be a consideration of the implementation planning process). It also stated that the introduction of IDN ccTLDs requires that a number of additional technical aspects be taken into account, in particular ensuring ongoing compliance to the IDNA protocol and IDN Guidelines. This need for ongoing technical compliance is also consistent with the notion of fast track deployment recognized by the IDNC WG.

As part of the implementation planning process, ICANN staff sought input and guidance from the community to develop a formal arrangement that included a general description of responsibilities for both ICANN and IDN ccTLD managers. This community input indicated that there should at least be a mechanism to ensure that all IDN managers adhere to the IDNA protocol over time, as well as compliance with associated standards, guidelines and other standards as they develop.

Taking into account the feedback received and guided by the direction set by the ICANN Board, ICANN staff prepared this paper on the proposed agreement between IDN ccTLD managers and ICANN. This topic is considered on two levels:

1. The need for a formal arrangement between an IDN ccTLD manager and ICANN.
2. The elements necessary to a formal arrangement.

ICANN is actively soliciting your comments on this important subject. This feedback will play a key role in shaping final implementation plans, intended for presentation at the ICANN meeting in Sydney (June 2009).

1. Need for a formal arrangement

As part of the planning for the implementation of the Fast Track process, ICANN has evaluated its current program to achieve stable agreements with country code top-level domain managers. Currently, ICANN is meeting this responsibility with its ongoing programme of voluntary Accountability Frameworks (AF).

Since ccTLDs were introduced the circumstances and environment has changed considerably. This includes an increasing demand for transparency and accountability, increased need to ensure the security and stability of the Internet for the benefit of the local and global community, and demand to delineate the roles and responsibilities of the entities involved in the function of the DNS.

The introduction of IDN ccTLDs will require that a number of additional technical aspects are taken into account to ensure the security, stability and resilience of the Domain

Draft—for discussion only—please refer to the disclaimer on the title page of this document.

Name System. In particular it will be necessary to ensure that the IDN ccTLD manager adheres to the IDNA protocol and IDN guidelines on an ongoing basis and until a full PDP process can be completed for cc IDNs.

The introduction of IDN ccTLDs under the Fast Track process is closely associated with the global IDN program, which also includes the introduction of IDN generic TLDs. This program is also developed through ICANN's bottom-up multi-stakeholder processes and in close cooperation with the technical community.

As part of this early introduction of IDNs it is required that some of the technical and operational aspects are accounted for to ensure the security, stability and interoperability of the Domain Name System. As noted previously, this is evident in the IDNC WG report and documented further in a note from Tina Dam, ICANN's IDN Program Director to Mr. Janis Karklins, chair of the GAC and Mr. Chris Disspain, chair of the ccNSO, included as Annex B. In this context it will be necessary to ensure that the IDN ccTLD manager complies with the IDNA protocol and the IDN guidelines on an ongoing basis.

Taking into account ICANN's mission to ensure the security, stability and interoperability of the DNS, the new technical environment and conditions associated with the introduction of IDNs and the relevant technical operational requirements, the fast track implementation plan proposes a "DoR" between the IDN ccTLD manager and ICANN.

The DoR is intended to document the roles and responsibilities of both the IDN ccTLD manager and ICANN, particularly to ensure adherence with the relevant standards and guidelines during the phase of fast track deployment and pending the conclusion of the IDN ccPDP (Policy Development Process for the longer term introduction of IDN ccTLDs, see <http://ccnso.icann.org/workinggroups/idn-pdp-process-time-table-02dec08.htm> for more information).

Consistent with current ccTLD practices, the IDN ccTLD manager will be responsible for developing and setting policies associated with the operation of the IDN ccTLD in accordance with national laws. The IDN ccTLD manager will not be required to abide by ICANN's consensus policies.

2. Proposed elements of the documentation of responsibilities

ICANN's relationship with ccTLD managers is currently formalized through the Accountability Framework program.

In December 2006, the ccNSO issued *Guidelines for ccTLD managers Accountability Framework discussions with ICANN*. The Guidelines were the result of considerable discussion within the ccTLD community over an approximate period of 18 months, and were the basis upon which ICANN developed the Accountability Framework templates. Under the current program, which is voluntary, a ccTLD manager can choose to sign either an exchange of letters or an accountability framework document with ICANN.

The proposed DoR has been modeled on, and is consistent with, the overall structure of an Accountability Framework; these frameworks have proven to be an acceptable and successful formal arrangement between many ccTLDs managers and ICANN. In preparing the DoR, the general principles and an overview of the clauses to be contained in the DoR have been discussed with a number of key players in the IDN ccTLD community, and have received in principle agreement. The proposed DoR is included in Annex A, and sections that are not similar, or are not contained in the Accountability Framework template, have been marked with an asterix (*).

Draft—for discussion only—please refer to the disclaimer on the title page of this document.

The DoR is tailored to focus on DNS stability and security, with an emphasis on adherence with independently derived technical standards and the IDN Guidelines.

The proposed DoR contains the following sections:

A. Background

This states the overarching principle that both ICANN and the IDN ccTLD manager want to demonstrate their commitment to maintain and enhance the security and stability of the DNS. It also confirms the delegation of the IDN ccTLD to the manager and provides a description of the relevant parts of the mission of both the IDN ccTLD manager and ICANN.

B. Mutual Recognition of Roles and Responsibilities

This section contains the recognition and acknowledgement of the roles and responsibilities of both the IDN ccTLD manager and ICANN.

C. Core Commitments

These commitments by both ICANN and the ccTLD manager are similar to the commitments agreed with ccTLDs under the Accountability Framework program, with the addition of specific commitments related to the operation of an IDN ccTLD. Given the fast track nature of IDN ccTLDs and, to ensure the interoperability, security and stability of the DNS in the interest of both the local and global users of the Internet, it must be ensured that the registration policy for the IDN ccTLD complies with the IDNA protocol and IDN guidelines.

D. Intellectual Property Rights

This is a statement that the delegation of the IDN ccTLD cannot be interpreted as granting an IP right in IDN ccTLD string.

E. Termination

These are mechanisms to terminate a DoR similar to the mechanisms contained in the Accountability Frameworks.

F. Effect of Termination

This sets out the impact of termination, in particular a mechanism to ensure that as much as can be reasonably expected under the circumstances, parties will continue to perform their roles to maintain stability, security and interoperability of the DNS. The Accountability Frameworks contain a similar section.

G. Cooperative Engagement

This contains a mechanism to ensure that ICANN and the IDN ccTLD will, as a first step, attempt to resolve any dispute in a cooperative manner.

H. Dispute Resolution Mechanism

This sets out a mechanism for resolving a dispute out of or in connection with the present agreement through binding arbitration by three arbitrators.

I. Exclusion of Monetary Liability

This section excludes either party from any monetary liability. The Accountability Frameworks contain a similar section.

Draft—for discussion only—please refer to the disclaimer on the title page of this document.

J. Exclusion of Transfer or Assignment of Obligations Under DoR

The DoR is only between the ccTLD manager and ICANN and cannot be transferred or assigned to another party.

K. Entire Agreement

The DoR contains everything that the parties have agreed.

Annex A

Proposed draft Documentation of Responsibilities – IDN ccTLD

Please note that the sections marked with an (*) are not similar to, or are not contained in the Accountability Framework template.

This Documentation of Responsibilities (DoR) is between:

[IDN ccTLD], an organization incorporated under the laws of the [country], in [location], hereinafter referred to as 'IDN ccTLD',

and

THE INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS, hereinafter referred to as 'ICANN', jointly to be referred to as: 'parties' and individually to be referred to as: 'party'.

A. Background

1. The parties want to demonstrate their commitment to maintain and enhance the stability, security and interoperability of the Internet's Domain Name System (DNS) from a global perspective and for the benefit of the local and global Internet community in an evolutionary manner on the basis of a peer relationship.
2. (*)The [.] Top Level Domain has been selected in [name of territory] in [year] and endorsed amongst others by the relevant public authority as a meaningful representation of the name of the territory.
3. The request for delegation of the [.] Top Level Domain was submitted by [IDN ccTLD] in [year] and [IDN ccTLD] is [legal status in country] and executes its operation in [country].

[IDN ccTLD] functions regarding the stability and interoperability of the DNS are to:

- Maintain and keep maintained name servers for the [.] domain;
 - Generate updates to [.] zone data when changes occur and propagate those changes to all public authoritative name servers for the [.] domain; and
 - Ensure continued and stable domain name system interoperability with the global Internet.
4. ICANN is responsible for providing technical-coordination functions for the management of the system of unique identifiers of the global Internet, including the DNS. Among ICANN's responsibilities is to oversee operation of the Internet's Authoritative Root Server System. As part of ICANN's responsibilities it:
 - a. Enters and maintains data in the Authoritative Root database and triggers updates of the root zone file.

Draft—for discussion only—please refer to the disclaimer on the title page of this document.

- b. Coordinates the allocation and assignment of the three sets of unique identifiers for the Internet, which are:
 - domain names (forming a system referred to as "DNS");
 - Internet protocol ("IP") addresses and autonomous system ("AS") numbers; and
 - Protocol port and parameter numbers.
- c. Coordinates the operation and evolution of the DNS root name server system.
- d. Coordinates policy development reasonably and appropriately related to these technical functions.

B. Mutual Recognition

1. Recognition of [IDN ccTLD]. ICANN recognizes [IDN ccTLD] as the manager and sponsoring organization of the [.] Top Level Domain, and the entity responsible for maintaining the [.] Top Level Domain, as a stable and interoperable part of the global domain naming system for the Internet in a manner that is consistent with [country] national law, public policy and naming policy.
2. Recognition of ICANN. [IDN ccTLD] acknowledges that ICANN is the entity responsible for maintaining and keeping the root of the Internet DNS stable and globally interoperable in a manner that is consistent with ICANN's Mission and Core Values as reflected in its bylaws.

C. Commitments

1. Commitments of ICANN.

ICANN shall use its best endeavors to:

- a) Authoritative-Root Database: maintain a stable, secure, and authoritative publicly available database of relevant information about [.] the Delegated IDN country code Top Level Domain, in accordance with ICANN publicly available policies and procedures. At the start of this DoR, the Authoritative Root Database shall contain information for the public authoritative name servers for [.] contact information for [IDN ccTLD], the designated administrative contact(s), and the designated technical contact(s) as notified to ICANN;
- b) Update of Name Server Information: implement on notification by the [IDN ccTLD] a change to the domain name or IP address(es) of the name servers for [.] as recorded in the Authoritative-Root Data for [.] in the Authoritative-Root Database according to ICANN's publicly available policies and procedures. The initial format and technical requirements for such a change are set out in ICANN's publicly available policies and procedures;
- c) Publication of Root-zone Whois Information: publish data maintained in the Authoritative Root Database about [.] which shall include at least the names of [IDN ccTLD] as the Sponsoring Organization, the administrative contact(s), the technical contact(s), and the domain names and IP addresses of the authoritative name servers for the domain;

Draft—for discussion only—please refer to the disclaimer on the title page of this document.

- d) Operation of Authoritative Root Server System: coordinate the Authoritative Root Server System so that it is operated and maintained in a stable and secure manner; and cause the Authoritative Root Server System to publish DNS resource records delegating the Top Level Domain [.] to the name servers recorded in the Authoritative Root Database and to inform the named administrative contact(s) and technical contact(s) of the published changes to the name servers for [.] .
- e) Maintenance of Authoritative Records and Audit Trail: maintain authoritative records and an audit trail regarding changes to [.] delegations and records related to those delegations and shall inform [IDN ccTLD] of the status of a requested change related to [.] in accordance with the policies, procedures and format as made publicly available by ICANN; and
- f) Notification of Contact Changes: notify [IDN ccTLD] of any changes to ICANN's contact information no later than seven days after the change becomes effective.

2. Commitments of [IDN ccTLD].

[IDN ccTLD] shall use its best endeavors to:

- a) Provision of zone data for [.] : generate regular updates of the [.] zone data in compliance with relevant standards as set out in paragraph c) and subject to and within the limits of relevant national law and national public policy.
- b) Provision of Name Service for [.] : operate and maintain the authoritative name servers for [.] in a stable and secure manner, adequate to resolve names within the [.] domain by users throughout the Internet and in compliance with Relevant Applicable Standards subject to and within the limits of relevant national law and national public policy. Relevant Applicable Standards are standards-track or best current practice RFCs sponsored by the Internet Engineering Task Force.
- c) (*) Adherence to relevant IDN standards and guidelines: register IDN domain names in accordance with its publicly available registration policy which shall comply on an ongoing basis with Relevant Applicable Standards to IDNs, such as the IDNA Protocol, and with the IDN guidelines as updated and published from time to time on the ICANN website, all subject to and within the limits of relevant applicable national law and public policy.
- d) Accuracy and Completeness of Information: notify ICANN, through ICANN's designated point of contact of:
 - any change of the contact information of its administrative or technical contact(s), and
 - any change to the administrative and /or technical contact details about [.] in the Authoritative-Root Database no later than seven days after the change becomes effective. The administrative contact for [.] must be directly associated with [IDN ccTLD] and must reside in the territory of [country].

Draft—for discussion only—please refer to the disclaimer on the title page of this document.

D. (*) No Conference of Intellectual Property Rights in IDN TLD String

Nothing in this agreement shall confer any intellectual property rights or preferences in the TLD string.

E. Termination.

This DoR may only be terminated in the following circumstances:

- There has been a determination by arbitration under Section H that a party is in violation of the DoR and that party continues to behave in the same manner for a period stated in the arbitration decision, or if no period is stated, twenty-one days;
- Either party will not or is unable to perform its duties under the DoR and has given written notice to such effect;
- In the event either party shall voluntarily or involuntarily be subject to bankruptcy or insolvency proceedings and such proceedings are not dismissed within 60 (sixty) days;
- By mutual consent of the parties; or
- By either party in the event that a re-delegation takes place, provided that in any re-delegation discussions the existence of this DoR shall be taken into account.

F. Effects of Termination

All obligations under this DoR shall cease. ICANN and 'IDN ccTLD Manager' are still obligated to perform their duties in accordance with this DoR to the extent this is within their powers and can be reasonably expected under the circumstances in order to maintain the stability, security and interoperability of the DNS.

G. (*) Cooperative Engagement

In the event of an activity or lack of activity that generates a serious concern regarding the stability, security and interoperability of the Internet's Domain Name System (DNS) from a global perspective or a disagreement between 'IDN ccTLD Manager' and ICANN arising under or out of this Agreement, either party may by notice to the other invoke the cooperative engagement provisions in this section.

If either party provides written notice to the other demanding cooperative engagement, then each party will, within 7 (seven) calendar days, designate a single executive officer as its representative to resolve the dispute.

The designated representatives shall, within 2 (two) business days after being designated, confer by telephone or in person to attempt to resolve the dispute.

If they are not able to resolve the dispute during such telephone conference or meeting, they shall further meet in person at a location mutually agreed to within 7 (seven) calendar days after such initial meeting, at which the parties shall attempt to reach a definitive resolution.

The time schedule and process may be modified with respect to any dispute, but only if Parties agree to a revised time schedule or process in writing.

Draft—for discussion only—please refer to the disclaimer on the title page of this document.

H. Resolution of Disputes

All disputes arising out of or in connection with the present agreement shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce by 3 arbitrators appointed in accordance with the said Rules. (*)Provided, however, that before either party may initiate arbitration as provided in this section, IDN ccTLD Manager and ICANN must attempt to resolve the dispute by cooperative engagement as set forth in the previous section G.

The arbitration shall be conducted in the English language.

If the Parties cannot mutually agree on a location, [PLACE, Country] shall be the default location, only following the failure to resolve the dispute pursuant to cooperative engagement.

There shall be three arbitrators: each party shall choose one arbitrator and, if the two arbitrators are not able to agree on a third arbitrator, the third shall be appointed by the ICC in accordance with its Rules of Arbitration.

Issues of law arising in connection with the interpretation of this DoR shall be resolved by the rules of law considered by the arbitrators to be most appropriately applied in all the circumstances; provided that the validity, interpretation, and effect of acts of [IDN ccTLD] and its legal status at the start of the dispute shall be judged according to the laws of [IDN ccTLD manager country] and the validity, interpretation, and effect of acts of ICANN and its legal status shall be judged according to the laws of the State of California, United States.

(*)The prevailing party in the arbitration shall have the right to recover its costs and reasonable attorneys' fees, which the arbitrators shall award.

(*)The decision of the arbitration panel shall be final and binding, and judgment may be entered in any court of competent jurisdiction.

I. No Liability

(*)The arbitrators shall have no authority to award consequential, incidental, indirect or punitive damages to either Party. (*) [IDN ccTLD Manager] and ICANN agree that irreparable damage could occur if any of the provisions of this Agreement are not performed in accordance with its specific terms. (*)Accordingly, the parties agree that they each shall be entitled to seek from the arbitrator's specific performance of the terms of this Agreement. No breach of an obligation under this DoR other than dispute resolution fees shall give rise to any monetary liability by one party to another. This Agreement shall not be construed to create any obligation by either ICANN or 'IDN ccTLD Manager' to any non-party to this Agreement.

J. Transfer or Assignment

No party may transfer, assign or sub-contract this DoR or any of its obligations under this DoR without the prior written consent of the other party.

K. Entire Agreement

This DoR contains the entire agreement of the parties in relation to the subject matter contained within it. No variation of this DoR shall be binding unless it is in writing and signed by both parties.

Annex B

Email Tina Dam to Janis Karklins and Chris Disspain

-----Original Message-----

From: Tina Dam
Sent: Tuesday, November 04, 2008 10:27 PM
To: 'Chris Disspain'; Jānis Kārklīņš
Cc: Donna Austin; Bart Boswinkel
Subject: IDN technical standards

Chris, Janis,

I understand that there were some questions yesterday around why the IDN technical standards should be complied with. Below please find a write-up on this topic. I cleared this last night with parts of the technical community.

Please share this with your respective communities and please let me know if there are any questions or anything I can do to address this further in person this week.

Tina

Tina Dam
Director, IDN Program
ICANN

Cell: +1-310-862-2026
Office: +1-310-301-5838

Why Compliance with IDN technical requirements are a necessity on a global scale:

Overall compliance with technical standards are important for TLD registry managers in order to keep their TLD stable and secure and in that way function and work well for their consumers and communities. Per ICANN Bylaws, interoperability of the Internet is a core value, which requires that technical standards are complied with. In some instances failure to comply with technical standards will only affects the corresponding TLD in isolation and does not interfere with other TLDs - when moving to the topic of IDN TLDs however this fact changes very quickly.

The following will demonstrate how non-compliance with IDN technical standards in one country or territory has a negative effect on the entire Internet community and not solely on that country/territory.

What history has shown us is that when IDNs are implemented in a manner not consistent with the IDNA protocol and IDN Guidelines it has a very negative effect on the community in general. For example, initially, under some TLDs, IDNs were implemented in a way that allowed the individual users and registrants to pick among characters across scripts when making their <IDN>.<ascii-tld> registration. This resulted in visual confusability and phishing attacks. One specific example of this is paypal.com, where the "a"s are Cyrillic characters and the rest are Latin letters. This

Draft—for discussion only—please refer to the disclaimer on the title page of this document.

address is visually the same as paypal.com (all in Latin letters), but physically, to the computer, these are two different addresses. This is damaging the uniqueness principle of the DNS - probably the most important principle of the DNS and what makes it work in a stable manner.

What further happened as a reaction to these kinds of implementations of IDNs is that application developers that need to implement the IDNA protocol in their application software in order for IDNs to work (for example in order for IDN based web addresses to resolve in a web-browser) did not follow the technical standards either. The reason behind this non-compliance has been an attempt to protect users from issues such as the above mentioned phishing attacks. For example, some browser developers have implemented white-listing of TLDs that have implemented IDNs, where the browser developer decides which TLDs are have implemented IDNs in a safe manner based on criteria set by the browser developer. As a result the end user is presented a variety of different implementations that aim at introducing security levels that really only can be implemented and need to be implemented at the root and TLD registry level. As a consequence if two TLDs support the same language and script, they also can accept the same 2nd level domains, and vice versa, if one lookup a domain name in Unicode in one TLD then one should be able to use the same software to look up the same Unicode domain name in a different TLD - however this will not always be possible. In other instances application developers have introduced mechanisms that prevent domain names in certain scripts from resolving or otherwise functioning adequately.

If IDN implementations continue down a road of non-compliance with IDN technical requirements, such as those present in the IDNA protocol and the IDN Guidelines, it will not be possible to determine what the level of damage will be for the end-user. The worst scenarios could be one of the following two: either that IDNs will be filled with phishing attacks that IDNs will be of no use and users will be scared of using them, or restrictions in the application layer will be so strict that IDNs will for example not resolve in an adequate and at least not in a stable and secure manner. Either way, this does not provide the community what they have asked for and what we are attempting to provide them with the implementation of IDNs, namely, equal access to the DNS by all languages and scripts.

Other examples can be provided on request. These relate to reasons why the IDNA protocol is under revision and are further documented in RFC4690.

In summary the above demonstrates why compliance with the IDN technical standards are of outmost importance, and why we need to find a way of ensuring that such compliance is in place and kept in place for TLD managers with IDNs implemented, regardless of whether it is a second level or top level.