IDN Variant TLD Implementation: Risks and Mitigation

25 January 2019

Table of Contents

Background

The current report is part of the six documents finalized and published after the public comment:

A. IDN Variant TLD Implementation – Executive Summary
B. IDN Variant TLD Implementation – Motivation, Premises and Framework
C. IDN Variant TLD Implementation – Recommendations and Analysis
D. IDN Variant TLD Implementation – Rationale for RZ-LGR
E. IDN Variant TLD Implementation – Risks and their Mitigation
F. IDN Variant TLD Implementation – Appendices (A: Glossary, B: Use of ROID, C: Limiting Allocated Variant TLDs)

Risks and Their Mitigation

Multiple risks for implementing the IDN Variant TLDs were identified in the earlier phase of this work, with varying degree of likelihood and severity. Based on the analysis, this report presents more details of the risks with a higher likelihood and severity. This report also discusses in more detail the potential mitigation which should be undertaken to address these risks.

1 Risk 1: No Agreement on the Definition of Variants

IDN variants must be identified before they can be implemented. If the identification of variants is left to the applicant, it would create arbitrary differences which can result in significant confusion and potential disputes. Therefore, a single source of rules is needed to determine valid TLDs and their variant TLDs. To address this need to have a single source, the community developed the Procedure to Develop and Maintain the Label Generation Rules for the Root Zone in Respect of IDNA Labels.

Because of the technical nature of the Unicode, DNS, and IDNA standards, and because of the inherent interest of linguistic communities in the labels that might be registered in the root zone, the LGR Procedure created a two-pass approach to creating the Root Zone Label Generation Rules (RZ-LGR). First, the LGR Procedure requires the community to organize into script-based Generation Panels (GPs) and propose relevant rules for the script. Once the proposal for a script is finalized by the GP after a public comment, it is evaluated by an Integration Panel (IP), which has expertise in linguistics, Unicode, domain name system (DNS) and IDNA. This second panel ensures that the GP proposal is technically sound based on the principles identified and that it also does not create potential problems, either in integration of other scripts and writing systems, or for the DNS more generally. Proposals which are successfully

evaluated are integrated into the Root Zone Label Generation Rules (RZ-LGR) by the IP. Each updated version of integrated RZ-LGR is again released for public comment before its finalization.

The overall LGR Procedure guiding the development of RZ-LGR has been developed by the community through a consultative process. Following the finalization of the LGR Procedure in 2013, a public call was made to invite the community members to organize into the various script-based GPs. Further, each of the component script-based LGR proposal is developed by the relevant script-based community group. The wider community also has multiple opportunities to provide input to the proposal by the GP at various stages through public comment process. However, even though these are result of a community based effort, the LGR Procedure and the resulting RZ-LGR are not part of the relevant IDN TLD policies created by the ccNSO and GNSO, because such policies were in place before the LGR Procedure was developed.

This situation needs to be rectified, which requires both GNSO and ccNSO to agree to integrate the RZ-LGR in their relevant policies and procedures.

For the GNSO this requires:

(i) implementing the RZ-LGR to define variant labels of the IDN gTLDs already delegated in the recent application round
(ii) incorporating the use of RZ-LGR to determine valid IDN gTLDs and their variant in the subsequent gTLD application rounds.

For the ccNSO this requires:

(i) updating the current IDN ccTLD Fast Track process to allow for the use of RZ-LGR to determine the variant TLD labels for applications already successfully evaluated
(ii) updating the current IDN ccTLD Fast Track process to allow for the use of RZ-LGR to determine valid TLD labels and their variants for subsequent applications through this process
(iii) incorporating the use of RZ-LGR to determine valid IDN ccTLD labels and their variants in the IDN country code policy (through IDN ccPDP), as a replacement for the current IDN ccTLD Fast Track process

It should be noted that having the RZ-LGR is a necessary but not a sufficient condition for the possible delegation of variant TLDs.

1.1 Risk

As there has to be a single RZ-LGR, GNSO, ccNSO and the technical community need to agree to use it to validate TLD labels and define variants of these labels. As the RZ-LGR has not been developed through the policy development process, the risk is that one or more of GNSO,

ccNSO or the technical community do not agree with the definition of variants as depending on the RZ-LGR and therefore do not incorporate it in the relevant TLD policies and procedures.

There may be one or more types of disagreement: (i) with the contents of the RZ-LGR finalized by a particular script community, (ii) with the underlying LGR Procedure itself, or (iii) with the scope of the RZ-LGR, e.g. limiting it to apply only for determining variant labels for TLDs, but not for validation of the applied-for TLD labels, especially for the scripts which have not been integrated into the RZ-LGR.

Any such disagreement by GNSO, ccNSO or the technical community will put the RZ-LGR approach in dispute. Depending on the level of disagreement, i.e. with the contents of the RZ-LGR or the underlying LGR Procedure, it may also entail that there will be no way to determine the variant labels of the existing and future TLD labels.

1.2 Mitigation

Currently the implementation of the RZ-LGR is being considered as part of the IDN variant TLD implementation. However, as has been discussed, the implementation is not possible without the definition of IDN variant TLDs. Therefore, it is suggested that the RZ-LGR implementation be separated from the IDN variant TLD implementation process and be made its pre-condition. It is justifiable because unless the community agrees what the variant labels of a TLD are, it is not possible to implement them.

This follows the ICANN Board resolution to implement the LGR Procedure, including updating the gTLD Applicant Guidebook and IDN ccTLD Process to incorporate RZ-LGR in the respective evaluation processes.

Therefore, a clear communication should be designed to the community for the following purposes:

(i) present the technical rationale behind developing and using the RZ-LGR
(ii) share the details of the community based process to develop the RZ-LGR, to highlight its participatory nature, transparency and conservativeness
(iii) clarify and explain that this is a necessary by not sufficient pre-condition for implementing variant TLDs, managing the expectations of the community
(iv) ask GNSO and ccNSO to adopt RZ-LGR in its relevant policies and procedures listed, sharing the implications of adopting the RZ-LGR
(v) reiterate the responsibility of the script communities in timely finalizing script-based LGR proposals for the Root Zone as a critical part of the process in developing the RZ-LGR, sharing implications of any delays
(vi) state the responsibility of the script communities in timely review and update script-based LGR proposals for the Root Zone in the future as a critical part of the process in maintaining the RZ-LGR and addressing any objections to it

Segregating the RZ-LGR adoption from larger process of implementing IDN variant TLDs and communicating that it be accepted as a pre-condition has multiple advantages:

1. Separating RZ-LGR adoption splits the IDN variant TLD implementation process into smaller parts. This also means that the associated risks are divided, allowing to focus on handling a subset of risks at a time, making the process more manageable.
2. Requiring RZ-LGR adoption as a pre-requisite involves the community earlier in the process, addressing the growing community concerns that there is need for progress on implementing variant TLDs.
3. Setting RZ-LGR as a pre-condition for implementing IDN variant TLDs also puts requisite pressure on the various active generation panels to finalize their work and submit their proposal for integration into the RZ-LGR.
4. Introducing the IDN variant TLD implementation process only after the RZ-LGR has been debated and accepted starts building a deeper level understanding and a more conservative level of expectation in the community for implementing the IDN variant TLDs.
5. Taking the process forward piecemeal simplifies the implementation process from the perspective of the community to understand and review, a better option from releasing all details simultaneously, as the latter option will be harder to grasp and address.

In addition, highlighting an objection process within the LGR Procedure, and allowing expansion of IP membership in such cases, where possible, can also help the community to agree with RZ-LGR calculations.

Finally, the community should be advised that a single solution must be agreed and recommended with the requisite endorsements from the different constituencies. The ICANN Board should consider lifting the ban on IDN variant TLDs only when there is evidence of very broad consensus and agreement from the GNSO and the ccNSO. Until this is achieved, the existing ban by the ICANN board should persist.

2 Risk 2: Same Entity Constraint Not Implemented by the Community

By definition, a TLD *t1* and its variant *t1v1* are considered the "same" by the community. This means that the domain names formed using the same second level label *s1* under these TLD variants, *s1.t1* and *s1.t1v1,* will be considered the "same" by the community as well. The community-based working group states in Integrated Issues report (IIR) that when resolving domain name, there are two failure modes:

a) **Denial of service:** the user attempts to visit http://example.Y, reading it as being the same as http://example.X … but connection does not work because … example.Y is not registered

b) **Misconnection:** the user attempts to visit http://example.Y, reading it as being the same as http://example.X … but arrives at a site controlled by a registrant different to that of example.X.

These failure modes are echoed by the Security and Stability Advisory committee in SAC 60. SSAC notes that misconnection causes worse results compared to denial of service because misconnection "presents issues of possible credential leakage, accidental disclosure of information, and user confusion and frustration" (SAC 60) and therefore should be avoided. SSAC further notes that "Confusability cannot be considered in isolation from other issues related to security. Phishing and other social engineering attacks based on domain name confusion are a security problem for end users" (SAC 089).

Therefore, based on the definition of the variants, the expectation of the community and the security implication, it has been proposed that *s1* be allocated to the same entity under all TLD variants or blocked, but it should not be possible to assign *s1* to different entities or registrants to prevent misconnection.

This imposes a requirement for the registries to ensure that there are relevant constraints and checks in registration process of a label under other TLD variants, if it has already been registered under one of them. In turn, this also has impact on the registrars, which manage these registrations. And finally, the registrants may also be impacted, where they may need to understand the concept, importance and consequences of registering and activating a label under different TLD variants.

On a related note, this binding will require that transfer of *s1* is managed across all TLD variants synchronously (if *s1.t1* is transferred, then *s1.t1v1* is also transferred) and that any other processes, e.g. dispute resolution, are also updated accordingly.

2.1 Risk

Due to the possible complexities involved, with implications and overhead on registration policy, operations, engineering and business, the GNSO or ccNSO community may not agree to the same entity constraint on *s1* under variant TLDs.

As a result, the expectation that the IDN variant TLDs are the "same" is violated from an end-user perspective and a label *s1* under TLD variants (*s1.t1* and *s1.t1v1*) may be allocated to different entities. This would cause misconnection for end-users with associated security consequences.

2.2 Mitigation

This requirement should be made part of the relevant policies and procedures for IDN variant TLDs by GNSO and ccNSO.

For existing gTLDs applying for variant TLDs, this should be explicitly included in the contractual terms for the IDN variant TLDs. Further the contract for the primary TLD already in place will need to be amended to support this requirement. Due to inclusion in policy and contracts, review for this function will be added to the regular compliance checks for IDN variant TLDs.

For gTLDs applying for primary TLDs along with the variant TLDs simultaneously, the same conditions would apply, except some additional checks may be needed for two undelegated TLD variants in parallel. If that is not technically feasible, then sequencing delegation of IDN variant TLD after the primary IDN TLD has been delegated should be considered as an alternative. This will not require additional checks.

It should also be required that this constraint be included and published as part of the publicly posted registration rules for primary TLD and its variant TLDs, to ensure that the registrants are aware of the requirement.

For IDN ccTLDs applying for variant TLDs, the ccNSO should be recommended to explicitly include the condition in the application process (e.g. agreed as commitment by the applicant in Fast Track evaluation application form). ccNSO should also be recommended to include intended registration rules for the requirement as part of the application for IDN ccTLDs and IDN ccTLD variants, so that this can be verified during the application evaluation step. IDN ccTLDs should also be encouraged to publicly post these registration rules for primary ccTLD and its variant ccTLDs to inform the registrants and the relevant community.

The registries should also require the additional condition from registrars for maintaining the same entity for a label under different IDN variant gTLDs during registration, transfer, dispute resolution and other relevant processes.

ICANN should work with ccNSO to determine ways to reach out and ask the ccTLD community to raise awareness of this need with their registrars and resellers.

3 Risk 3: A Combinatorial Explosion of Domain Names Due to Variants at Top and Other Levels

While discussing the IDN variant TLDs, it is stated in the Integrated Issues report (IIR) that "A cautious approach should be adopted; successively more liberal approaches may be adopted later … The goal should be … to minimize active entries".

This is noted by the SSAC, which states that "Variants introduce a permutation issue both at the top level as well as with combinations of top level and second level … assume a TLD string with four characters, where each character has three variants … [and] assume a 2LD string with four characters, where each character has three variants … Thus the variant set created would be 3^4 x 3^4= 72171. Such large number of variant strings presents challenges for the management of variant domains at the registry, the registrar and registrant levels. Conservatism is also to be used in this case for the root as well. … The SSAC agrees with the recommendations [that]… A variant TLD application must be accepted only if the TLD applicant clearly demonstrates the necessity for activating the string. Variants that are not necessary, but are desired, must not be allocated and activated" (SAC 60).

Therefore, a coherent policy should be developed which can identify and prioritize the needed labels from the allocatable pool of labels generated, noting that the procedure for "a variant management mechanism could encompass both active use of labels in the DNS, and prevention of labels from use in the DNS" (IIR).

3.1 Risk

A large number of variant labels for a large number of candidate TLDs in the future could generate a large number of labels in the root zone. Beneath those variant labels could arise a large number of variant labels as well, leading to a combinatorial explosion of many different names that all need to be managed together. This could demonstrate the significant operational overhead implied by variants to operations of the DNS, EPP, WHOIS/RDAP, registrar operations, web site configurations (handling large number of same site identifiers), web browsers, mail administration, and so on.

This could also create a backlash against IDNs or variants.

3.2 Mitigation

Integrated Issues report (IIR) hints at the possible mitigation measures which can be designed. It suggests that TLD variants should be limited "to those where an explicit need has been established, the user experience implications have been fully studied, and no [or minimal] negative impacts to security or stability have been identified". This suggests three criteria for selecting which of a variant TLD should be delegated: (i) need, (ii) usability, and (iii) security and stability. SSAC agrees that "The approval of a variant TLD must not be automatic, but initiated upon the request of a TLD applicant, explicitly specifying … the need for the variant (e.g., motivated by linguistic, security, usability and/or other considerations)" and suggests that "A string that is allocatable does not imply automatic activation; rather that it can be allocated … a clear process needs to be developed to avoid ad hoc treatment of new gTLD applications" (SAC060).

Based on the reasons and recommendations shared, both the ccNSO and the GNSO should be asked to develop conservative criteria based on need, usability and other considerations to determine which IDN variant TLD label may be applied-for. The criteria may be different for ccNSO and GNSO as both have different guiding requirements, e.g for an IDN ccTLD variant to be successfully evaluated, should it also meaningfully represent the same country or territory for the relevant community? The relevant policy and procedures should include these criteria in the evaluation process of a IDN variant TLD.

Further, to prevent a combinatorial explosion across multiple levels, for the TLDs which have activated variants at the top-level, it should be recommended that these TLDs and variant TLDs should develop a conservative second level policy for labels and their variants, which should (i) reduce automatic activation of variant domain names to whatever is appropriate but no more than what is necessary, and (ii) Reduce registration of variant domain names to whatever is

appropriate but no more than what is necessary. Moreover, to help with the management of possible combinations of domain names, the registered second level labels should be kept consistent and predictable under all active variant TLDs. The ccNSO and GNSO should be asked to consider specifying these additional policy recommendations.

4 Risk 4: Proposed IDN Variant Policy and Procedure Changes Not Endorsed Widely

Community has indicated need for IDN variant TLDs through both the gTLD and IDN ccTLD application process. However, due to lack of a clear definition and a solution to implement them, ICANN Board resolved on 25 September 2010 that "no variants of gTLDs will be delegated through the New gTLD Program until appropriate variant management solutions are developed." Follow up work reported in IIR identified that "[in] the DNS environment today, there is no accepted definition for what may constitute a variant relationship between top-level labels, nor is there a 'variant management' mechanism for the top level".

The RZ-LGR, being developed using a community based LGR Procedure, provides the definition of the variant labels for a TLD for the script which have been integrated. The additional report on *Recommendations for Implementing the IDN Variant Top Level Domains (TLDs)* suggests a "variant management mechanism" which is the second part of the requirement in the ICANN Board's resolution.

These recommendations will be finalized in consultation with the Board IDN Working Group. Based on the direction of the ICANN Board, the finalized recommendations would need to be presented to the community for adoption. The recommendations provide guidance on how variant TLDs should be implemented, and will need to be incorporated in the relevant policy and procedures by the GNSO and the ccNSO. These recommendations may further change based on the community feedback, once the report is released publicly. A consistent set of guidelines must be agreed and adopted for all TLD variants, irrespective of them being country codes or generic names. Only then the ban imposed by the ICANN Board should be released. Otherwise, the ban on IDN variant TLDs should continue.

It should be noted here that this second step can only occur after RZ-LGR has been adopted as a source of definition of variants of the IDN TLDs (see mitigation of Risk 1 above).

4.1 Risk

There is a possibility that one constituency agrees to the recommended approach, and another does not (e.g. GNSO agrees and ccNSO does not, or some ccTLDs refuse the approach, and so on) but the approach is implemented anyway. In that case, a certain amount of user confusion appears likely (both among consumers and among registrants of domains).

4.2 Mitigation

The risk can be addressed if there is clear communication that recommendations are based on the fact that TLD variants are being delegated, and country codes and generic names and fundamentally both TLDs.

To ensure a solution agreed by all the stakeholders, it may be useful to invite experts and develop a single cross-community consensus to review the recommendations and send a single collective assessment to the supporting organizations and advisory committees for adoption. This should include technical experts to ensure that any proposed changes by the working group remain technically coherent.

5 Risk 5: Variant Set Broken by a Court of Competent Jurisdiction

Variant TLD labels are by definition considered the "same" by a script community. To meet this expectation, it is recommended that the variant TLDs must be allocated to the same entity or blocked. Otherwise, as noted by SSAC and discussed in Section 2.1 above, due to the confusion between labels which are considered variants of each other, end-users may face misconnections which can create security issues for them.

The current recommendations suggest that if one TLD undergoes a change in the entity to which it is allocated, the same change should be applied for all other allocated variant TLD labels. This change could occur through any of the processes supported by ICANN, e.g. Registry Transition Process or Change of Control. Same is applicable in the event that a TLD's operations are transitioned to any Emergency Back-End Registry Operator (EBERO).

However, even if this recommendation is implemented by the ICANN community and integrated into the relevant policies and procedures for TLDs, a court of competent jurisdiction may still rule to split one of more variant TLDs from a variant TLD set created by the RZ-LGR. This may occur for any number of reasons, e.g. as a result of a trademark dispute. In such cases the assumption of TLD variant set being managed by the same entity is broken, allowing registrations for the same label under the TLD variants *s1.t1* and *s1.t1v1* by different registrants at the second level, and consequently potentially creating a misconnection security risk for end-users.

5.1 Risk

A court of competent jurisdiction rules against the disposition of variant labels created by the RZ-LGR and either separates two variants from one another or establishes an alternative definition of "variant" TLD. This could happen for multiple reasons, e.g. due to Trademark dispute.

5.2 Mitigation

Motivation, reasoning, relevant documentation and contractual requirements are all relevant details which any court of law would consider before ruling in any case. Therefore, to mitigate the risk for this possibility of a court breaking a variant TLD set, appropriate documentation of

technical reasons behind the LGR Procedure, the open objections process at the time of application and contractual clauses should be developed and integrated in the relevant policy and procedures. The documentation should also provide the risks at-large, to the user community, in case a TLD set is broken, for submission in such court cases. Support of the wider community should be documented for the requirement. And, the legal team should be involved in drafting and reviewing the documentation to ensure all the relevant aspects are covered with proper legal reasoning. This expectation for TLD variants should be widely communicated during the application process to ensure the implications are understood by the community and this evidence of openness can be presented in the court of law.

In addition, the processes at the time of application and afterwards, which deal with trademark issues related to the TLDs could be revisited and expanded in scope to include other IDN variant TLD set, in addition to the applied-for TLD.

Finally, if the community agrees, a new reserved state of a label, beyond “allocatable” and “blocked” (e.g. “policy-blocked”), can be defined through policy for use in such a dispute. If a court of law breaks a variant set, this could be implemented by making the split sub-set “policy-blocked” which would separate the sub-set from the original applicant and put it in this reserved category. First-come-first-served rule can be used to argue that this subset cannot be allocated or delegated, as is for other reserved labels. Though it will break the variant TLD set, but will prevent the new subset from being allocated to a different entity by making it reserved, reducing the adverse impact.

6 Risk 6: “Same Entity” Requirement Will Not Have Consistent Implementation

At the second level and below, ensuring the same label beneath all variant TLD labels are allocated to the same entity could be achieved using multiple mechanisms, e.g., having the same ROID for the registrant. Because the ROID is generated by the repository, it is guaranteed to refer to the same contact object in the registry. However, a practical consideration with this option is that some registrars in practice may not reuse contact objects for different registrations. If this option were to be used, registrars would need to support the requirement. Also, ccTLDs that do not implement EPP must identify the "same entity" by some other mechanism. It is important to note that depending on heuristic matches of data fields generated by humans tends to be subject to errors introduced by those humans, so it is better to identify common data based on a unique identifier of some sort (i.e. something functionally equivalent to a contact object ROID in EPP).

6.1 Risk

The “same entity” rule will not have consistent implementations, leading to more creeping differences among different IDN implementations.

6.2 Mitigation

ICANN should work with GNSO to find effective mechanisms, e.g., to reuse ROIDs for the same registrant in case of IDN variant TLDs. This may be included through the policy and resulting contractual requirements, and verified using the compliance mechanisms.

ICANN should work with ccNSO to request its members to use a consistent mechanism for this purpose, e.g., EPP and ROID. Also, for cases ROID is not used by the ccTLDs, the ccNSO may be requested to develop a common definition of "same entity" based on a well-defined subset of the registration data and encourage its members to adopt it consistently, in case they implement IDN variant TLDs. In this case, further guidelines may also need to be developed to ensure that variation caused due to human interaction can be managed for the short-listed fields, e.g. by automatically duplicating information for the selected fields rather than a manual re-entry; this should also include automatic updates to all tied records, in case one is changed. Though this will be different from the implementation of ROID, it will still help reduce arbitrary implementations and resulting inconsistencies.

Another alternate is to have a single "shared" registration data record for such registrations. However, this would require developing an appropriate technical mechanism to manage, and is not clear if the technical community will agree to such a mechanism, especially because ROID mechanism already exists.

7 Risk 7: IDN Variant TLD Implementation Adversely Impacts Universal Acceptance

The community is already facing a challenge of universal acceptance of domain names[1]. This is introduced for domain names which are new, or longer than the anticipated length, or because they are IDNs. Introduction of variant TLDs will impose more expectations by the end-users, which would need technical updates to existing software tools and applications. A detailed analysis of user experience due to the introduction of IDN variant TLDs, presented in the report on Examining the User Experience Implications of Active Variant TLDs, shows that it can put significant additional burden on the application providers (see section 6.4 of the report). Already taxed by the existing challenge of universal acceptance due to IDNs, this additional burden due to the IDN variant TLDs could be the last straw, causing the application providers to stop supporting the IDNs or to refuse extending support for the variants of IDN TLDs effectively, worsening the universal acceptance challenge.

7.1 Risk

Implementation of variant TLDs may exacerbate the universal acceptance challenge due to differing implementations and user expectations. Software vendors and tool providers (e.g. web browser and mail user agent developers) decide that this recommended approach is inadequate and reject IDNs (or IDNs that generate many variants) as too dangerous or difficult to implement.

[1] See www.uasg.tech for further details regarding the universal access challenges.

7.2 Mitigation

Early outreach on the need, policy, implementation details and implications of variants of IDN TLDs on universal acceptance would help mitigate the impact. This outreach should focus separately on end-users to clarify what they can expect from implementation of variant domain names. In addition, communication material will separately need to be developed for application providers to address anticipated challenges.

Trying to address these challenges in sequence, after the universal acceptance of IDNs has been addressed, may also help reduce the burden on the application and tool providers. This could be addressed by deploying IDN variant TLDs after a reasonable progress on universal acceptance of IDN TLDs has been made.

In case such delay is not acceptable for the community, it may still help keeping a conservative outlook on implementation by minimizing the number of variant TLDs delegated at the outset. This may help in containing the challenges associated with the implementation of variant TLDs.

8 Risk 8: IDN Tables and Variant Labels at the Second Level Not Managed by the Community

As the TLD *t1* and its variant *t1v1* are considered the "same" by the community, second-level label *s1* and its variant *s1v1* are also considered the "same". So the discussion on failure modes and security implications for misconnection is also applicable to second-level variant labels (see details in Risk 2 discussion above). Therefore, it has been proposed that IDN tables under the variant TLDs be harmonized to create consistent variant labels at the second-level and that the variant labels *s1* and *s1v1* generated using these IDN tables be allocated to the same entity under all TLD variants or blocked. It should not be possible to assign *s1* and *s1v1* to different entities or registrants under any of the variant TLDs to prevent misconnection.

This imposes requirements for the registries to ensure that there are relevant constraints and checks in the IDN tables and in registration process of all variant labels under TLD variants. In turn, this also has impact on the registrars, as they have to manage the constraints on who can register second-level variant labels. And finally, the registrants may also be impacted, where they may need to understand the concept, importance and consequences of registering and activating variant labels under different TLD variants.

On a related note, this binding will require that transfer of *s1* is managed across all second-level and TLD variant labels synchronously (if *s1.t1* is transferred, then *s1.t1v1, s1v1.t1* and *s1v1.t1v1* are also transferred) and that any other processes, e.g. dispute resolution, are also updated accordingly.

8.1 Risk

As this is related to the registration policy for the second-level, community may consider this as out of scope of ICANN's mandate. Also, due to the further complexities involved, with implications and overhead on second-level registration policy, operations, engineering and business, the GNSO or ccNSO community may not agree to harmonize IDN tables or agree to the same entity constraint on *s1* and its second-level variant labels under IDN variant TLDs.

As a result, the expectation that the IDN variant TLDs are the "same" is violated from an end-user perspective and a label *s1* and its variant labels under TLD variants (*s1.t1*, *s1.t1v1, s1v1.t1* and *s1v1.t1v1*) may be allocated to different entities. This would cause misconnection for end-users with associated security consequences.

8.2 Mitigation

To manage criticism regarding the mandate of ICANN, it should be clearly communicated to the community that these pertain to the security and stability considerations which is ICANN's mandate to address. Further, these requirements also follow from the updated (draft) version of the IDN Implementation Guidelines developed by the community and are essential for secure use of IDNs at the second level.

For existing gTLDs applying for variant TLDs, harmonization of IDN tables and same entity constraint for second level variant labels should be explicitly included in the contractual terms for the IDN variant TLDs. Further, the contract for the primary TLD already in place will need to be amended to support this requirement. In addition, to verify that the variant labels at the second-level are harmonized, the IDN tables for all relevant IDN variant TLDs should be submitted for testing. Due to inclusion in policy and contracts, review for this function should be added to the regular pre-delegation testing and compliance checks for IDN variant TLDs.

For gTLDs applying for primary TLDs along with the variant TLDs simultaneously, the same conditions as above would apply, except some additional tests may be needed for two undelegated TLD variants in parallel, in case the tests require checking against an already delegated TLD. If that is not technically feasible, then sequencing delegation of IDN variant TLD after the primary IDN TLD has been delegated should be considered as an alternative.

It should also be required that these constraints be included and published as part of the publicly posted registration rules for primary TLD and its variant TLDs, to ensure that the registrants are aware of the requirement. This publication requirement has already been included for the second-level variant labels in the updated (draft) version of the IDN Implementation Guidelines.

For IDN ccTLDs applying for variant TLDs, the ccNSO should be recommended to explicitly include the condition in the application process (e.g. agreed as commitment by the applicant in Fast Track evaluation application form). ccNSO should also be recommended to include intended registration rules for the requirement as part of the application for IDN ccTLDs and IDN ccTLD variants, so that this can be verified during the application evaluation step. IDN ccTLDs

should also be encouraged to publicly post these registration rules for primary ccTLD and its variant ccTLDs to inform the registrants and the relevant community.

The registries should also require the additional condition from registrars for maintaining the same entity for a label under different IDN variant gTLDs during registration, transfer, dispute resolution and other relevant processes.

ICANN should work with ccNSO to determine ways to reach out and ask the ccTLD community in order to raise awareness of this need with their registrars and resellers.

It should be noted that until the security aspects for IDN Variant TLDs are not addressed, the ICANN Board may not lift the ban on them.

9 Risk 9: Tools to Manage IDN Variant Domain Names Not Available

IDN variant domain names are available today in limited numbers because variant labels are only permitted at the second level. Delegating IDN variant labels at the top level will have a much more significant impact, as it will create potential variant domain names for each registration under the TLD. ICANN has received a public comment noting that "even though variant label registrations at the second level have been available for many years, there are still no commonly used tools to create common DNS records for variant zones, nor to configure web, mail, or other application servers to provide consistent responses for variant names. Often variant names are unconfigured or misconfigured, creating poor or misleading user experiences." A more detailed analysis is also presented in the user experience study on the potential impact of active IDN variant TLDs.

The community has identified that support for variant domain names needs to be enabled by a variety of stakeholders in a variety of applications. Such updates to applications are needed, for example, so that variant labels may be "easily deployed as clones, easily transferred to new owners and operators en bloc, and easily verifiable to be the same by a policy auditor,"[2] as noted in a public comment. It is anticipated that tools will be needed to manage this potential prevalence of variant domain names. In addition, tools will specifically be needed to manage the top-level variant labels, as these will be delegated for the first time.

9.1 Risk

With the potential proliferation of IDN variant domain names, sufficient tools may not be available for managing and using the variant domain names effectively, creating a risk for registries, registrars, registrants and end-users.

[2] Comment by Business Constituency during the public comment.

9.2 Mitigation

As discussed, variant domain names have been available at the second level, so there is some experience, expertise and tools available for managing them. Further, experience and implementations of bundling are also available at the top-level for some ccTLDs and one pair of gTLDs, which can inform the implementation of IDN variant TLDs. However, with further proliferation of IDN variant domain names due to IDN variant TLDs, more focus is needed by the community on developing and updating relevant tools and applications. As (i) there is no single solution proposed by the technical community for bundling domain names, and (ii) the needs of various script communities for using IDN variant domain names may vary, more work is needed to determine what are feasible implementation mechanisms for the tools and applications.

To help mitigate the risk, it will be useful to document how the community currently manages the variant domain names. It may also be useful to put together a guide for best practices for managing IDN variant domain names, to assist the development of effective tools and applications. Where relevant, the work may be taken up within the Universal Acceptance initiative. Finally, a communication strategy should be developed to share these documented practices and guidelines with the relevant stakeholders, e.g. the application developers, to apprise them of the potential impact of IDN variant domain names and how to address it.