A Case Study and Evaluation of a Sample Risk Mitigation Plan

To demonstrate how Risk Mitigation Plans should be developed and evaluated under the amended Fast Track Implementation Plan and proposed risk Mitigation Guidelines, the joint ccNSO and SSAC working party has analysed the case of .eu in Greek (.ευ/.EY) and evolution of the IDN ccTLD Fast Track process.

This analysis is also intended to serve as input for the overall IDN ccTLD policy review. In time, after updating the proposal and after adoption by the Board and implementation the recommended policy is expected to replace the IDN ccTLD Fast Track process.

Introduction of Risk Mitigation Measures in the Fast Track Process

Since its introduction in 2013, the Extended Process Similarity Review Panel (EPSRP) reviewed three cases (one in Cyrillic and two in Greek script) and published its findings in September 2014.[1]

The EPSRP found that one of the applied for Greek strings should be considered confusingly similar with 2 two-letter codes *in upper-case*, and should not be considered confusingly similar to any combination of two ISO 646-Basic Version (ISO 646-BV) characters or with existing TLDs, applied for TLDs or reserved names *in lower-case*: "[…] The proposed new DNs to evaluate (in several fonts, in both uppercase and lowercase) are ευ/EY in Greek. […] In the case of EU, EY (Greek upper case) -EV and EY (Latin upper case) comparisons exceeded the threshold criterion in all cases, and so the decision to reject is clear."

In June 2015, following the public review of the implementation of the Extended Process Similarity Review Panel (EPSRP), the ICANN Board of Directors requested the ccNSO, in consultation with other stakeholders including the Governmental Advisory Committee (GAC) and the Security and Stability Advisory Committee (SSAC), to provide further guidance on and refinement of the methodology of the second string similarity review process, including the interpretation of its split recommendations.

In January 2017, the ccNSO submitted the requested guidance and refinement to the Board, which was based on the ccNSO EPSRP working group Final Report.[2] The SSAC produced SAC 084,[3] 088[4] and 089.[5]

In April 2017, following submission of documents by the ccNSO and SSAC, the ICANN Board of Directors suggested that the ccNSO and SSAC should further collaborate to reach a common understanding and way forward on their views with respect to the following three areas:[6]

1. RFC 6912
2. Similarity Evaluation findings
3. Mitigation measures

---

[1] See: https://www.icann.org/resources/pages/epsrp-reports-2014-10-14-en.
[2] See: https://ccnso.icann.org/workinggroups/epsrp-final-report-27sep16-en.pdf.
[3] See: https://www.icann.org/en/system/files/files/sac-084-en.pdf.
[4] See: https://www.icann.org/en/system/files/files/sac-088-en.pdf.
[5] See: https://www.icann.org/en/system/files/files/sac-089-en.pdf.
[6] See: https://www.icann.org/en/system/files/correspondence/crocker-to-sataki-faltstrom-24apr17-en.pdf.

The ccNSO and SSAC created a small, informal group (Working Party) to address the questions of the Board. This Working Party developed a common position and both the SSAC and the ccNSO Council approved this document, which then submitted to the Board in September 2017.

In light of its observations and recommendations, the Working Party proposed changes to section 5.6.3 of the FT Implementation plan by including the opportunity for the intended manager: to "propose, agree upon and implement adequate pre-arranged risk mitigation measures with the goal to reduce the potential risk of user confusion as of the moment the IDN ccTLD becomes operational, including specific consideration of confusability from the perspective that any domain name may be displayed in any case (lower- or upper-case), depending on the software application and regardless of the user's familiarity with the language or script". In addition, "to determine whether the proposed risk mitigation measures are adequate ICANN will consult experts in the area of relevant Risk Mitigation measures and the IDN ccTLD string requestor. The proposed measures are to be evaluated together with the finding of the confusability evaluation."

The Working Party also suggested that the recommended overall policy for the selection of IDN ccTLD strings should be amended accordingly.

At its meeting on 29 October 2017, the Board approved the proposed refinement of the string similarity review of the IDN ccTLD Fast Track Process as suggested by the joint ccNSO-SSAC Working Party and the President and CEO, or his Designee(s), is directed to incorporate the amendment into the Implementation Plan.

In December 2017, the President of ICANN's Global Domain Division informed the ccNSO and SSAC that, as part of the implementation, ICANN organization developed draft guidelines to evaluate the risk mitigation measures as well as the selection criteria of an external panel that would conduct the evaluation. The joint ccNSO-SSAC Working Party was requested to provide feedback and input on draft guidelines.

Risk Mitigation Guidelines and Case study

Following the request of ICANN organisation, the joint ccNSO – SSAC Working Party developed and propose a set of Guidelines for the Risk Mitigation Process under the IDN ccTLD Fast Track Process, based on and taking into account the Guideline as originally proposed by ICANN Organization. The ccNSO-SSAC Working Party Guideline is included in a separate document. To test the proposed Guideline and provide a basis for testing the amended Fast Track process, the joint working party conducted a case study.

Proposed Risk Mitigation Plan

According to the EPSRP, the requested string εu is deemed confusingly similar to two 2-lettter combinations EV and EY[7] . One of these 2-letter strings (EV) is reserved for use in standard ST.3[8] and not available as TLD. The other 2-letter combination (EY) is currently unassigned[9] . Therefore, the .εu

[7] See EPSRP Report: https://www.icann.org/en/system/files/files/epsrp-european-union-30sep14-en.pdf
[8] According the ISO On Line Browsing Platform the code element EV is indeterminately reserved. See: https://www.iso.org/obp/ui/#search
[9] See: https://www.iso.org/obp/ui/#search

is deemed confusingly similar with two strings that are not in use as TLDs. This aspect might be worth assessing based on international standards of risk.

Based on the ISO 31000 standard, the definition of RISK is “the effect of uncertainty on objectives”.

Analyzing the risks of confusing similarity of the .ευ to 2 two letter combinations that could be used as ccTLD strings and using a security-based risk assessment, it can be concluded that:

1. The vulnerability is “visual confusing” between 2 non-related domain names.
2. The threat would be “abusing the visual confusing similarity” for malicious purposes (mostly phishing).
3. The occurrence of this threat is, at present, ZERO, as the codes have not been assigned yet. In the future, the occurrence might exist.
4. The risk is undefined, but it can be assumed that it is limited to financial and maybe reputational risk. Quantifying this risk is even more difficult as it depends on the targeted domain names (one could assume a worst case scenario, but this implies taking a high profile, non-existing, domain name – an equivalent of paypal.com/amazon.com/facebook.com in this specific name space) that would be abused.
5. The resulting assessment would be that the risk would be, at present, ZERO, and in the future close to zero, should these codes be assigned.

There are four ways of treating risks:

1. AVOIDANCE: avoid any action that would cause the risk.
2. REDUCTION: implement mitigation (this only reduces the risk, and the relation between the mitigating action and the quantified risk is extremely difficult to calculate).
3. TRANSFER: transfer the risk to another party (e.g. insurance).
4. ACCEPTANCE: one can accept the risk.

From a risk assessment point of view, it is worth highlighting the following elements:

1. Abusive DN registrations are a fact.
2. Abusing visual similarity (aka homographs) is a known vulnerability.
3. The risk exists, but is limited (homographs are a very small portion within the risk of phishing attacks).
4. It is possible to reduce risks through some measures.
5. By reviewing the assessment yearly, or when specific events happen (like adding a new TLD), it is possible to take into account the threat evolution and propose new mitigating techniques.

Conclusion
From a risk assessment perspective, assigning the .ευ is not an issue as the risk does not exist today and has little chance to exist and eventually affect anyone in the future.

To address possible identified risks, EURid, the registry of the .eu and .ею (.eu in Cyrillic) that manages the said ccTLDs on behalf of the European Commission, and requester of the string has produced a Risk Mitigation Plan that is based on several key principles.

- *Principle 1: One and only registry manager of .eu, .ею and .ευ*

Following the ccNSO resolution 68-02 of 26 October 2011 to amend the IDN Fast-Track Implementation Plan and the letter from Elise Gerich, Vice-President of IANA, dated 14 December 2011, on 13 January 2012 the European Commission sent a letter to IANA-ICANN to confirm that “the registry manager of .eu and the requested IDN ccTLD are one and the same entity, and will continue to be so in perpetuity”.

This measure is meant to ensure that possibly confusing similarities between the IDN ccTLD and the ASCII TLD are managed by the same entity, and eventually prevented.

- *Principle 2: Homoglyph bundling*

Homoglyphs are characters that, due to similarities in size and shape, might appear identical at first glance. The homoglyphs below represent two unique characters belonging to two different scripts, or alphabets:

Cyrillic character а → Unicode number 0430
Latin character a → Unicode number 0061

With the introduction of the so-called "homoglyph bundling" procedure for the .eu in any script, domain names that might look confusingly similar are prevented from being registered. This means that several domain names are bundled at one time, and none of the other domain names in that bundle can be registered.

More information about the homoglyph bundling procedure under .eu is available at https://eurid.eu/en/register-a-eu-domain/domain-names-with-special-characters-idns/

- *Principle 3: No mixing of script policy*

The script of the second level domain name must match the script of the TLD extension. For the existing scripts (.eu, .ею) it means that if the domain name being registered is in Latin script, the script at the top-level will be .eu. On the other hand, if the domain name being registered is in Cyrillic script, the script at the top-level will be .ею. A registrar wishing to register an exclusively numeric domain name – possibly including hyphens – should specify the TLD extension during registration. In the case that the extension is not specified, the .eu extension will be set by default.

The "no mixing of script" policy will also be enforced for the .ευ string. That means that Greek script domain names registered under .eu will be carefully and gradually transitioned to the .ευ string (see next principle).

- *Principle 4: Transition of IDN domain names under their corresponding script*

As of 1 June 2016, EURid has fully enforced the basic rule that the second-level script must match the top-level script, in order to eliminate any possible confusion. Domain names registered in Greek script are managed under the .eu rules at present. However, they will be affected by the "no-mixing of script" policy as soon as the .ευ string is delegated.

EURid will develop an administrative and communication strategy similar to the one currently in place for transitioning Cyrillic domain names under .ею which is reported below. Please note that since the introduction of the .eu in Cyrillic, no cases of abuse have been reported to EURid.

For domain names registered in Cyrillic under .eu, EURid has:

- Informed all registrars and registrants of the changes;
- Introduced a 'script adjustment' phase, to allow registrars and registrants to adopt domain name(s) where the top-level domain script matches the second-level domain script. The 'new' domain names under the Cyrillic extension have an initial term of three years free of charge until 31 May 2019. The switch ('cloning') was made under EURid's supervision during the maintenance window when .ею went live on 1 June 2016. All Cyrillic domain names were 'cloned', a process whereby the Latin extension was replaced with the Cyrillic extension, and

all linked contacts were copied. Name server information and DNS key information were not copied, as this information depends on the DNS setup of the registrar.

Consequently, EURid activated all Cyrillic domain names that had been cloned from .eu to .ею. The original and cloned domain names will now co-exist till 31 May 2019, and are maintained by the registrar independently of one another. During the script adjustment phase, registrars do not have to pay for cloned domain names. A 'cloned' domain name – meaning a Cyrillic domain recreated to be identical in terms of registrant and registrar data, but now with the Cyrillic extension – behaves as any other domain name would. Thus registrars can put the 'cloned' domain name into quarantine. The domain name will then be released after 40 days if not reactivated or transferred out of quarantine. All the special statuses, such as 'seized', 'withdrawn', 'on hold', etc., also work. With that being said, a new domain name cannot be re-registered as long as the 'original' – otherwise known as 'legacy' – Cyrillic domain name under the .eu extension still exists, as homoglyph bundling does not take the extension into account until the respective legacy domain name has been deleted. At the end of the three-year term, all legacy domain names will be deleted by EURid unless the registrar or registrant has already done this beforehand.

When the registrar deletes the original Cyrillic domain name under the .eu extension, it cannot be registered again, as it would break the 'no script mixing' rule.

- *Principle 5: Cooperation with EUIPO, CERT-EU, Europol for abuse detection and prevention*

During the last decade EURid has established strong partnerships and/or entered into MoU with several organisations that are regularly reporting abuses in the TLD environment. Should the .ευ string be delegated, EURid could further liaise with those entities to be notified immediately in case of abuses.

No cases of abuses linked to possible confusing similarity have been reported to EURid to date.

Further measures in case .EV and .EY are activated as country code

- The registry of the .ευ would seek to enter into a MoU with the registry of .ey and/or .ev. to foster cooperation procedures to prevent and/or mitigate possible confusing similarity (e.g. with the MoU, EURid may commit to enforce the bundling with any Greek.ey or Greek.ev, so that any registered Greek.ey or .ev will trigger the impossibility of registering the Greek.ευ equivalent).
- EURid would introduce a fast-track domain name suspension – similar to the current one within its Whois Quality Plan[10] – in case of reported abuses.
- Periodic assessment of the .ευ namespace from a security perspective carried out by an independent expert.
- Annual evaluation of the Greek domain names portfolio, possible abuses and report to the European Commission and ICANN about it.

Conclusion of the Working Party

The Working party has reviewed the case of eu in Greek, analysed the proposed Risk Mitigation Plan, and has concluded that the proposed and already implemented (for eu in Cyrillic) measures address

[10] The EURid Whois Quality Plan foresees a fast-track to suspend domain names with alleged abuses in three days from the date of the notification to the registrant and registrar.

the identified risks and mitigate them to the level that does not exceed risks of similar abuse in already existing TLDs.