EURid

EURid

Risk Mitigation Plan

Proposed Risk Mitigation Plan

On behalf of the European Commission, EURid applied through the ICANN IDN ccTLD Fast Track process in 2009 for the requested string .ευ (.eu in Greek script).

On 29 March 2019, ICANN announced the release of the updated IDN ccTLD Fast Track Final Implementation Plan (FIP), including changes proposed by the Joint ccNSO SSAC Response[1] as approved by the ICANN Board on 29 October 2017[2].

In accordance with the updated FIP, EURid now proposes risk mitigation measures which it undertakes to implement on or before the launch of the .ευ TLD. These risk mitigation measures have been prepared in accordance with international standards of risk, as foreseen by the Joint ccNSO SSAC Response.

In a report dated September 2014 by an expert panel appointed under the then ICANN IDN ccTLD Fast Track process (the Extended Process Similarity Review Panel or EPSRP), the requested string ευ in upper case was deemed to be confusingly similar to two 2-lettter combinations EV and EY[3]. The string was not considered to be confusingly similar to any ISOC 3166-1 entries.

With regard to the upper case strings, one of these 2-letter strings (EV) is reserved for use in standard ST.3[4] and not available as TLD. The other 2-letter combination (EY) is currently unassigned[5]. Therefore, the .ευ is deemed confusingly similar with two strings that are not in use as TLDs, neither is it anticipated that they will be in use as TLDs in the foreseeable future.

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 similarity” 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

[1] https://ccnso.icann.org/sites/default/files/field-attached/epsrp-final-response-17aug17-en.pdf
[2] https://www.icann.org/resources/board-material/resolutions-2017-10-29-en#2.c
[3] See EPSRP Report: https://www.icann.org/en/system/files/files/epsrp-european-union-30sep14-en.pdf
[4] According the ISO On Line Browsing Platform the code element EV is indeterminately reserved. See: https://www.iso.org/obp/ui/#search
[5] See: https://www.iso.org/obp/ui/#search

taking a high profile, non-existant, 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 under any extension.
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 by adopting appropriate measures.
5. By reviewing the assessment yearly, or when specific events happen (for example, following the launch of 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 of existing or affecting any internet user 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 . ευ 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 a ccNSO Council resolution 68-02 of 26 October 2011 to amend the IDN Fast-Track Implementation Plan and a letter dated 14 December 2011 from Elise Gerich, then Vice-President of IANA, 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 intended to ensure that risk of visually confusing similarities between the IDN ccTLDs .ею and .ευ and the ASCII TLD .eu are effectively mitigated by being managed by the same entity.

- *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 TLDs 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 by different registrants.

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 2 has been enforced for the .eu environment since the .*ею* string was launched on 1 June 2016. To date, no abuse and/or complaint have been reported to EURid.

- *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 with the Cyrillic extension, .ею – behaves like 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 to a different entity 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.

The proposed transition of existing second level Greek script IDN domains under .eu to the proposed .ευ IDN TLD has been successfully implemented under .ею. No complaints or claims of confusing similarity have arisen in practice.

- *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 MoUs 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 abuse linked to possible confusing similarity relating to IDNs have been reported to EURid to date.

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

In the unlikely event that the strings .EV and .EY are in the future delegated as a country code, EURid the registry for the .eu TLDs will take the following steps:

- EURid 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[6] – in case of any reported abuse.
- 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.

[6] 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.