Suggestions for NIS 2.0 Implementation Guidance to Achieve the Goals of the European Union Regarding TLD Name Registries and Entities Providing Domain Name Registration Services under Articles 21 and 28

By Michael Palage[1]

1.0 Executive Summary

The European Union's ground-breaking requirements on the domain name industry under Articles 21 and 28 in its revised Directive on Network and Information Systems (NIS2) are set to be transposed into member state law by October 17, 2024. To achieve the EU's stated goals of ensuring "the security, stability, and resilience of the DNS, which in turn contributes to a high common level of cybersecurity across the Union," the EU has a short window to drive meaningful improvements through targeted implementation guidance and the publication of best practices. Such guidance should be welcomed by the domain industry, which is currently struggling to understand how to adapt its current practices to comply with NIS2.

This document provides actionable guidance for E.U. Member States as they work to implement the NIS 2.0 Directive 2022/2555 under their respective national laws regarding "TLD name registries and entities providing domain name registration services" under Articles 14, 21, and 28. This guidance considers harmonizing with existing E.U. laws (GDPR, DSA, eIDAS, bankruptcy, etc.) and advancing President von der Leyen's broader vision for a European Digital Decade.[2]

As described in detail below, the following recommendations are suggested to harmonize the requirements under Articles 21 and 28 across the domain name industry:

- All domain names registered by a TLD name registry and entities providing domain name registration services shall publicly identify the registrant as either a natural or legal person.
- If the TLD name registry or entity providing domain name registration services permits privacy/proxy registration services, it shall identify the beneficial user/customer as the contact administering the domain name and their status as either a natural or legal person.
- TLD name registries and entities providing domain name registration services shall establish and abide by administrative processes to permit third parties to contest various aspects of domain names registered within that TLD, e.g. accuracy of all registrant data fields outlined in Article 28, access to non-public domain name registration data in the case of illegal/abusive activities, the registration and use of the domain name by an alleged natural person, etc. These administrative processes need to be publicly posted on the website of each TLD name registry and entity providing domain name registration services.

[1] Michael Palage is an intellectual property attorney and an information technology consultant with a Bachelor of Science in Electrical Engineering from Drexel University and a Juris Doctorate from Temple University Beasley School of Law. Mr. Palage has been actively involved in Internet Governance and ICT issues for over two decades. He has been intimately involved in ICANN operational and policy matters since its formation in both an individual and leadership role, including a three-year term on the ICANN Board of Directors. Mr. Palage most recently served as the Chair of ICANN's Registration Data Accuracy - Scoping Team.

[2] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

- TLD name registries and entities providing domain name registration services must provide differentiated[3] public access to the required data fields listed in Article 28 corresponding to the registrant type (e.g., natural/legal person).
- TLD name registries shall maintain a complete set of registration data (as required by NIS 2) in a dedicated database for that TLD.
- TLD name registries and entities providing domain name registration services shall take affirmative steps to identify any suspect registrations (e.g. inaccurate registration data or potential abuse) to flag for subsequent investigation/verification. Any registration flagged by a TLD Name Registry or entity providing domain name registration services shall undergo enhanced verification, e.g. eIDAS level "substantial."[4]

2.0 Problem Statement

While the domain name industry has discussed the impact of NIS 2.0 at length,[5] most of the discussion within the ICANN community[6] has failed to consider the following two fundamental issues. First, the ease with which bad actors can quickly register and use a domain name in connection with illegal activity and the corresponding difficulties for third parties in investigating and stopping this activity. Second, the direct link between the false and inaccurate registration data and its impact on the security of the broader domain name supply chain.

3.0 A Case Study to Illustrate the Shortcomings of Today's Registration Data

Drawing on the inspiration that a picture is worth a thousand words, the following registration data for the domain **icannsdefinitionofaccuracyisajoke.com** demonstrates the shortcomings of the current ICANN contractual requirements and the need for NIS 2.0. The table below lists the registrant information provided to the reseller (Unstoppable Domains) and the publicly available information available from the Registrar (region) and Registry (Verisign) respective WHOIS/RDDS service.[7] Since this initial registration, Unstoppable Domains has obtained ICANN registrar accreditation.

---

[3] Differentiated access means providing automated responses to queries based upon the credentials of the requestor (e.g. law enforcement, researcher, etc) and the type of registrant (natural v legal person).

[4] eIDAS is an EU regulation governing "electronic identification and trust services for electronic transactions. eIDAS provides three levels of identity proofing: low, substantial and high.

[5] CENTR has published a whitepaper on data accuracy (https://www.centr.org/news/news/data-accuracy-paper.html) and a related policy update on NIS 2.0 (https://www.centr.org/news/blog/icann76-whois.html); Palage, Michael, *NIS 2.0 and Its Impact on the Domain Name Ecosystem*, CircleID; https://circleid.com/posts/20240522-nis-2.0-and-its-impact-on-the-domain-name-ecosystem; Rickert, Thomas, *Demystifying Art. 28 NIS2*, CircleID, https://circleid.com/posts/20240609-demystifying-art-28-nis2; Marks, Dean, Alternative Insights on Article 28 of the NIS2 Directive, CircleID, https://circleid.com/posts/20240612-alternative-insights-on-article-28-of-the-nis2-directive.

[6] It is important to note when discussing the global domain name marketplace, the distinction between how gTLDs and ccTLDs have responded to the obligations imposed by NIS 2.0 directive.

[7] Regton's publicly available WHOIS/RDDS is available here - https://regtons.com/en/login/whois/ and Verisign's publicly available WHOIS/RDDS is available here - https://webwhois.verisign.com/webwhois-ui/c

	Unstoppable Domains Reseller (Not Publicy Available)	regtons Registrar (Publicy Available)	Verisign Registry (Publicly Available)
Name	Rock Key	Domain Admin	Not Provided (Thin Registry)
Organization	N/A	Whois protection, this company does not own this domain name	Not Provided (Thin Registry)
Address	E Tusculum St 1818 Philadelphia, PA 19134 US	Jaurisova 515/4 Praha 4, 14000 CZ	Not Provided (Thin Registry)
Email	icannsdefinitionofaccuracy isajoke@proton.me	icannsdefinitionofaccuracyisajoke.com@whoisprotection.domains	Not Provided (Thin Registry)
Phone	1.555-555-5555	420.2265174	Not Provided (Thin Registry)

This fake registrant information was inspired by the fictional character Rocky Balboa, played by Sylvester Stallone in the iconic movie franchise Rocky. The given name and surname were chosen as they are common Western names that ICANN does not consider patently inaccurate.[8] The address provided is a valid address, but it is a location where filming took place for the original Rocky movie. The telephone number is a syntactically valid but non-functional number associated with the U.S. country code. The valid email address icannsdefinitionofaccuracyisajoke@proton.me was a single-use disposable email address registered for the purpose of this experiment. The entire registration process took approximately 10 minutes using a pre-paid American Express card through the domain name reseller Unstoppable Domains.[9]

ICANN Org and the ICANN Registrar Stakeholder Group (RrSG) have both corresponded with the Network and Information Systems Cooperation Group Work Stream for art.28 NIS2, touting the robustness of the multistakeholder model and how they believe that NIS 2.0 aligns with existing ICANN domain name registration practices.[10] The RrSG earlier this year posted on its website a document entitled “RrSG Approach to Registration Data Accuracy.”[11] Sadly, however, the registration data associated with the domain name "icannsdefinitionofaccuracyisajoke.com" would be deemed “accurate” under the current definition agreed upon by the ICANN Registration Data Accuracy Scoping Team Deliberations and Findings for Assignments #1 and #2, which found:

---

[8] *Registration Data Scoping Team Deliberations & Findings for Assignments #1 and #2* (2 September 2022), see footnote #3 (page 12 of 52) https://gnso.icann.org/sites/default/files/policy/2022/correspondence/palage-et-al-to-gnso-council-rda-assignments-et-al-05sep22-en..pdf

[9] https://unstoppabledomains.com/blog/categories/announcements/article/unstoppable-offers-com

[10] ICANN Org Communication (9 November 2023), see https://itp.cdn.icann.org/en/files/government-engagement-ge/icann-policies-procedures-requirements-art-28-nis2-directive-09-11-2023-en.pdf and Registrar Stakeholder Group Communication (16 February 2024), see https://rrsg.org/wp-content/uploads/2024/02/RrSG-lette-re-NIS2-art-28-16-February-2024.pdf

[11] https://rrsg.org/wp-content/uploads/2024/03/RrSG-Approach-to-Registration-Data-Accuracy-March-2024.pdf

Under the current requirements, as spelled out in the Registrar Accreditation Agreement (RAA) as well as Consensus Policies, domain name registration data should be accurate, reliable, and up-to-date. Accuracy requirements are understood as entailing *syntactic* validation of the registration data elements provided by the Registered Name Holder or Account Holder as well as the verification of *operability* of either the telephone number or the email address.

To be determined to be syntactically valid, the contact must satisfy all requirements for validity (see Whois Accuracy Program Specification Sections 1b-d). For example, for email addresses all characters must be permissible, the "@" symbol is required, and there must be characters before the "@" symbol.

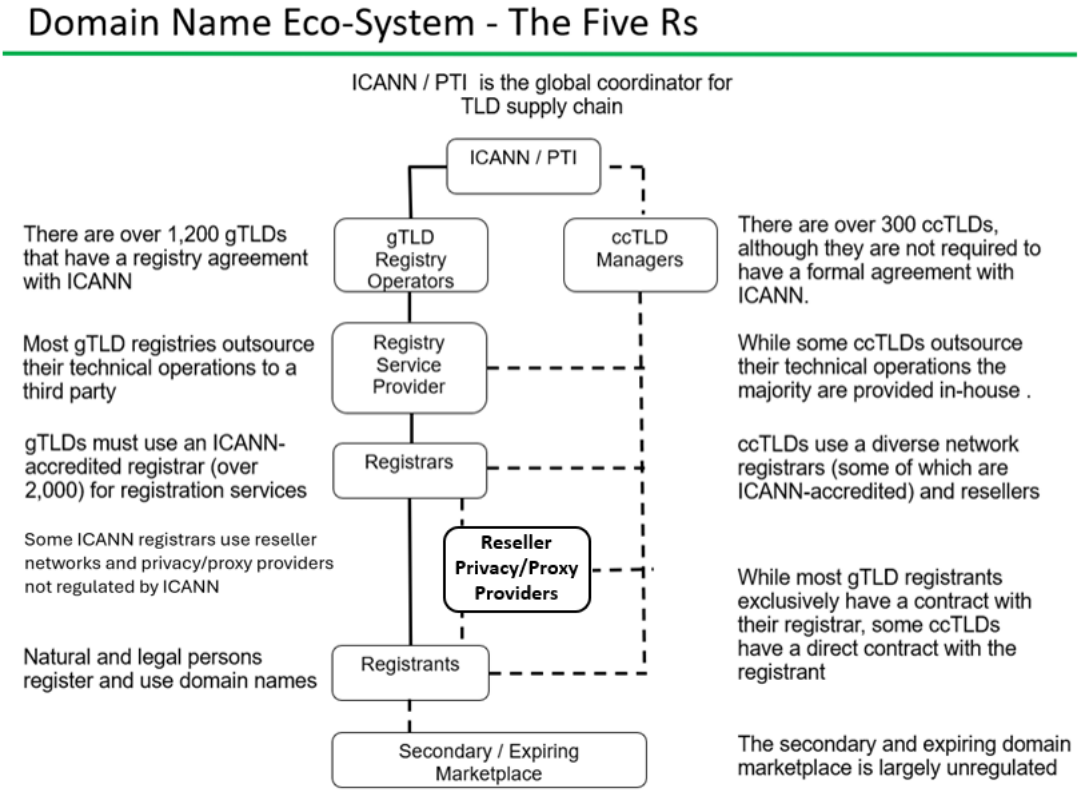
To be determined to be verified as operable, the contact must be operable as defined in the Whois Accuracy Program Specification Section f including an affirmative response from the Registered Name Holder for either email or phone.[12]

4.0 Domain Name Ecosystem Fundamentals

Before transposing the NIS 2.0 Directive into respective Member State law, it is important to understand the dynamics of the current global domain name ecosystem. The complexity of the DNS ecosystem and the challenges it poses for legislatures was noted in a recent Organisation for Economic Cooperation and Development (OECD) paper entitled *Security of the Domain Name System (DNS)*.[13]

The domain name system was first conceived by Paul Mockapetris in 1983. The first commercial domain name registration was made in 1985. In 1998, the year in which the Internet Corporation for Assigned Names and Numbers (ICANN) was incorporated as a California nonprofit public benefit corporation, there were approximately 4 million domain names registered globally.[14] This included both generic top-level domains (gTLDs), such as .COM, .NET, and .ORG, as well as country code top-level domains (ccTLDs), such as .DE, .FR, and .BE.[15] Today the number of global domain name registrations exceeds 362 million.[16] An overview of the current major stakeholders in this marketplace are illustrated in the diagram below.

[12] https://gnso.icann.org/sites/default/files/policy/2022/correspondence/palage-et-al-to-gnso-council-rda-assignments-et-al-05sep22-en..pdf (page 12 of 52).
[13] OECD (2022), "Security of the Domain Name System (DNS): An introduction for policy makers", *OECD Digital Economy Papers*, No. 331, OECD Publishing, Paris, https://doi.org/10.1787/285d7875-en.
[14] https://www.zooknic.com/Domains/counts.html
[15] The delegation dates of each TLD (gTLD or ccTLD) can be found online via the IANA database, see https://www.iana.org/domains/root/db
[16] Verisign Domain Name Brief, see https://dnib.com/listing/report



One of the most important things to note in this diagram, specifically regarding Article 21 (Cybersecurity risk-management measures) is that neither resellers nor privacy/proxy providers have a direct contractual relationship with ICANN. This unregulated part of the domain name supply chain further obfuscates the beneficial domain name user/customer. Unfortunately, ICANN has been unable over the last decade to implement policies to provide a legal framework for these types of service providers.

A recent ICANN Privacy and Proxy Services Accreditation Implementation call highlighted the direct and real impact that unregulated resellers and privacy proxy providers have on the security within the domain name supply chain.[17] Gabriel Andrews, a Governmental Advisory Committee (GAC) representative to the ICANN Implementation Review Team, asked a clarifying question about the respective roles of resellers and privacy proxy providers. Reg Levy, Associate General Counsel at Tucows made the following statement, "The majority of our resellers operates as a um like their customers think that they are a registrar**, they do not display the ICANN logo but in all other respects they act as though they are a registrar**." (emphasis added)

This statement by Levy, is consistent with the author's own experience when registering the domain name **icannsdefinitionofaccuracyisajoke.com.** Unstoppable Domains, in their capacity as a reseller at the time, acted as though they were a registrar. However, attempts by the author to identify which ICANN-accredited registrar they were using during the registration process were unsuccessful. The identity of the ICANN-accredited registrar was only discovered after the domain name was registered.

[17] https://community.icann.org/pages/viewpage.action?pageId=367362107 (relevant exchange occurred at the 35th minute of the Zoom recording).

To fully appreciate the scope of this unregulated reseller component in the domain name supply chain, one needs to look no further than Tucows Domains network of 35,000 resellers across 200 countries.[18] These dynamics and shortcomings highlight the need for supply chain security measures under Article 21, Paragraph 2.d, as described below in more detail.

While there are no exact figures on the actual overall size of the domain name marketplace, one of the more detailed analyses was recently published by three Massachusetts Institute of Technology (MIT) researchers who, in their paper, Changing Markets for Domain Names: Technical, Economic, and Policy Challenges, estimated the DNS ecosystem-related revenue to be approximately $8 billion annually.[19]

The secondary domain name marketplace[20] is currently estimated to be around $2 billion annually. Unlike the primary gTLD domain name market where ICANN has several well-established policies and direct contractual relationships with most of the relevant stakeholders, there is substantially less oversight and/or regulation by ICANN involving the secondary domain name marketplace. A secondary domain name marketplace has long been recognized within the industry and was first detailed in a 2006 OECD paper entitled *The Secondary Market for Domain Names*.[21]

Article 28 Considerations

4.0 Important Distinction Between gTLDs and ccTLDs

Because the NIS 2.0 Directive refers to "TLD name registries and entities providing domain name registration services" it is important to highlight the important distinctions between gTLDs and ccTLDs. Although gTLDs and ccTLDs are largely the same in terms of their technical operation, their governance structure and policies differ significantly from ICANN's governance of gTLD's and can also differ substantially among themselves. As illustrated in the diagram above, gTLD registry operators generally have a direct contractual relationship with ICANN, with the exception of .MIL, .EDU, and .GOV.[22] However, most ccTLD Managers have no formal contract with ICANN, instead opting for a lightweight Exchange of Letters or an Accountability Framework.[23]

These ccTLD Managers have a variety of governance relationships with their respective national governments and local internet communities. One example is the .FI ccTLD, where the Finnish Transport and Communication Agency Traficom is designated as the ccTLD Manager. There are also several ccTLDs in which the operation of the ccTLD is delegated to a private sector entity under a competitive tender by the government.[24] And, there are private sector-led arrangements where the ccTLD Manager may be a

[18] https://ir.tucows.com/wp-content/uploads/Tucows-final-10-K-04.01.24.pdf (Page 6)
[19] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3746594
[20] The secondary domain name marketplace involves the resale of an existing domain name, and may or may not involve an ICANN contracting party. The primary market generally involves interactions with ICANN contracting parties, e.g. Registrars and Registries.
[21] OECD (2006), "The Secondary Market for Domain Names", *OECD Digital Economy Papers*, No. 111, OECD Publishing, Paris, https://doi.org/10.1787/231550251200.
[22] https://www.icann.org/en/registry-agreements
[23] https://www.icann.org/resources/pages/cctlds/cctlds-en
[24] See for example . FR. and .EU.

cooperative or a not-for-profit private association of key local internet stakeholders, such as with .DE, .CZ and .UK.

The DNS Research Federation (DNSRF) recently published a research paper entitled *Habits of excellence: why are European ccTLD abuse rates so low?*, which reported: "E.U. ccTLDs have the lowest abuse rates of any TLD block within the global market."[25] The DNSRF also found "a correlation between E.U. ccTLD low abuse rates and the widespread adoption of diverse data quality measures among the E.U. ccTLDs."[26] While the DNSRF research paper discussed some of the contractual requirements for gTLDs regarding data retention models (e.g., "thick WHOIS" versus "thin WHOIS"[27]), it unfortunately did not examine one operational reality in today's domain marketplace.

Most ccTLDs operate a "thick WHOIS" data set in which the ccTLD Manager maintains access to the entire registration data set, including the identity of the actual beneficial registrant.[28] This is critically important for enabling a ccTLD Manager to better respond to legitimate inquiries from local law enforcement agencies and third parties concerning specific domain names. This "thick" WHOIS data also allows ccTLD Managers to use algorithms and machine learning to proactively identify suspicious domain name registrations and flag them for further registrant verification. Unfortunately, most gTLDs, even those that ostensibly maintain "thick WHOIS" data, **DO NOT** have access to information involving the actual beneficial user of the domain. This is because, in most cases, their "thick WHOIS" data set is comprised mainly of proxy and privacy registration data which is of de minimis value to legitimate access seekers in time-sensitive matters.[29]

Recommendations:

4.1 Member States should coordinate with their national ccTLD Manager to determine and document local best practices[30] for registration data verification and access processes for legitimate access seekers.

4.2 In transposing NIS 2.0 into national law, Member States should ensure that gTLDs operating in that Member State meet or exceed the data verification requirements and timely access to the same beneficial user data as that of the local ccTLD Manager. If the gTLD

[25] https://dnsrf.org/blog/habits-of-excellence--why-are-european-cctld-abuse-rates-so-low-/index.html
[26] IBID
[27] Traditionally , "thick" WHOIS referenced TLD name registries and entities providing domain name registration services that maintained a full set of registration data, e.g., Registrant Contact RoID and Administrative Contact RoID, as well as technical data (name servers), whereas "thin" WHOIS referenced TLD name registries and entities providing domain name registration services that maintained a minimum set of registration data, e.g. primarily technical data.
[28] In many cases, ccTLD Manager prohibits the use of privacy and proxy registration services. Beneficial registrant refers to the registrant who derives the benefit of using that domain name, as opposed to the individual or organization the domain name may be registered to.
[29] The registration data associated with the domain name registration ICANNSDEFINITIONOFACCURACYISAJOKE.COM lists the Registrant Name as Domain Manager, and the Organization as Whois Protection.
[30] Recital 111 of NIS 2.0 states that "TLD name registries and the entities providing domain name registration services should adopt and implement proportionate procedures to verify domain name registration data. Those procedures should reflect the best practices used within the industry and, to the extent possible, the progress made in the field of electronic identification."

operating in that Member State cannot meet the standards of the local ccTLD Manager, Member States should require in their national law additional safeguards (discussed below) for these gTLD name registries.

5.0 The Evolving Domain Name Ecosystem: Alternative Roots, Blockchains & Web 3.0 Domains

Web 3.0 and blockchain alternative naming services currently market themselves to internet users as providing "domain name" registration services.[31] Today, there are several ICANN-accredited registrars and domain name resellers that concurrently provide domain name registration services for both ICANN-delegated TLDs as well as alternative naming service TLDs.[32] However, these alternative naming service TLDs do not fit neatly within the current NIS 2.0 definition. For example, Paragraph 23 of Section 6 specifically references the "delegation of a specific TLD." While ICANN has a defined process for the delegation and transfer of TLD name registries, some alternative naming service TLDs claim to be self-sovereign and therefore may not involve delegation from a third party. Additionally, the operation of some alternative naming services may not require certain technical aspects enumerated in the definition, e.g. name servers, zone files, etc.

Recommendations:

5.1 Member States should consider the following revised definition:

'top-level domain name registry' or 'TLD name registry' means an entity which has been delegated or claims the right to operate a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, which may include ~~including~~ the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers, irrespective of whether any of those operations are carried out by the entity itself or are outsourced, but excluding situations where TLD names are used by a registry only for its own use;

5.2 Member States should include a specific reference in the NIS 2.0 national legislation to include alternative name services so that there is no potential gap in the protection afforded to internet users. This will also help minimize potential confusion with other provisions of the NIS 2.0 text which co-mingle references to TLD name registries and DNS services associated with the IANA Root Server System.[33]

---

[31] By way of example, Unstoppable Domains is the reseller where the domain **icannsdataaccuracyisajoke.com** was registered, see https://unstoppabledomains.com/. This website commingles the registration of both Web 2.0 and Web 3.0 domains. Since the original registration of this domain name, Unstoppable Domains has become an ICANN accredited registrar.

[32] ICANN accredited registrars providing Web 3.0 domain name registration services include EnCira (https://www.encirca.com) and NameCheap (https://www.namecheap.com/).

[33] Recital 32 references TLD name registries and "recursive domain name resolution services."

6.0 Defining Accuracy

Article 28 of NIS 2.0 requires "TLD name registries and entities providing domain name registration services to collect and maintain accurate and complete domain name registration data in a dedicated database." While this requirement and its intent are clear, ICANN's multistakeholder model has missed the mark with respect to its own accuracy definition requirements. As a result, it is up to the Member States to define accuracy to ensure that the legal standard for compliance is higher than required by ICANN.

In 2021, ICANN commissioned a Data Accuracy Scoping Team to undertake preliminary research and fact-finding regarding related policy work involving the collection and processing of domain name registrant data.[34] Unfortunately, after approximately one year of debate, the Scoping Team failed to reach a consensus on the definition of accuracy, which prevented ICANN from conducting further policy work on accuracy.[35] As a result, under ICANN's contracts, the registrant data provided in connection with the domain **icannsdefinitionofaccuracyisajoke.com** is compliant with the accuracy requirement outlined in the RAA even though it is very obviously fake.

The second issue with ICANN's approach to "accuracy" is its inadequacy with respect to Recital 112. This recital discusses the collection, processing and access to domain name registration data and states in relevant part:

> TLD name registries and entities providing domain name registration services should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. Those policies and procedures should take into account, to the extent possible, any guidance and the standards developed by the multi-stakeholder governance structures at international level.

Failure of Member States to provide a more useful definition of "accurate" could result in ICANN defaulting to the current RAA requirements, which as demonstrated above in connection with the **icannsdefinitionofaccuracyisajoke.com** domain name, is woefully inadequate.

Recommendations:

6.1 All TLD name registries and entities providing domain name registration services shall proactively analyze all domain name registrations (including the domain name itself and the full registration data set) to identify any suspect registrations, e.g. bulk registrations, keywords, suspect data, etc. Any domain name registration flagged as suspect shall undergo enhanced registrant verification at a "substantial " level outlined in applicable eIDAS regulations. Such TLD name registry or entity providing domain name registration services shall retain proof of such identity proofing.

6.2 All TLD name registries and entities providing domain name registration services shall ensure that any domain name flagged as suspect through a credible thirty-party report has undergone enhanced registrant verification at a "substantial " level outlined in applicable

[34] https://community.icann.org/display/AST/Registration+Data+Accuracy+-+Scoping+Team
[35] https://gnso.icann.org/sites/default/files/policy/2022/correspondence/palage-et-al-to-gnso-council-rda-assignments-et-al-05sep22-en..pdf (Page 12 of 52)

eIDAS regulations. Such TLD name registry or entity providing domain name registration services shall retain proof of such identity proofing.

7.0 Natural Persons Versus Legal Persons as Registrants

Article 28, Paragraph 4 states that "TLD name registries and the entities providing domain name registration services to make publicly available, without undue delay after the registration of a domain name, the domain name registration data which are not personal data." This appears to be an indirect way of stating that TLD name registries and the entities providing domain name registration services should make a distinction between natural and legal registrants. However, any potential ambiguity is removed by reading Recital 112 which states that for "legal persons, the TLD name registries and the entities providing domain name registration services should make publicly available at least the name of the registrant and the contact telephone number. The contact email address should also be published, provided that it does not contain any personal data, such as in the case of email aliases or functional accounts."

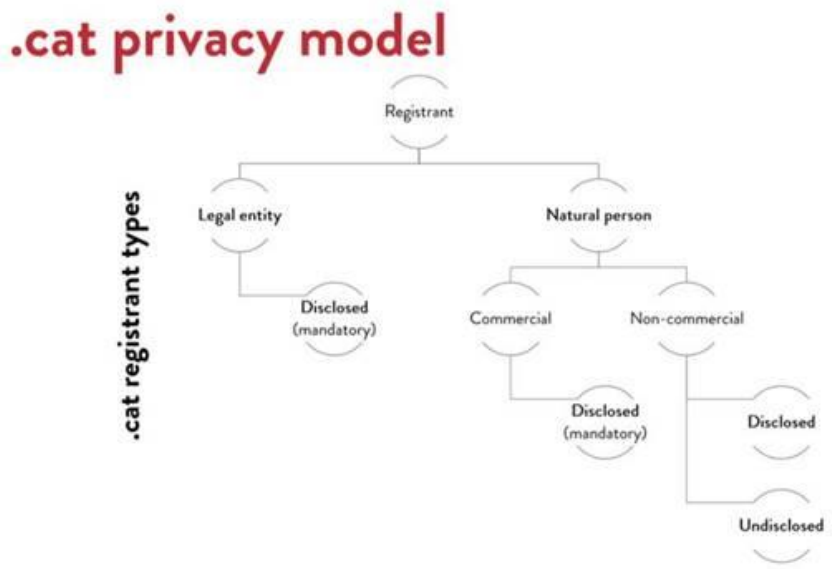
Over 70% of European ccTLDs currently distinguish between natural and legal persons as registrants when a third party does a RDAP/WHOIS query for domain name registration data.[36] This is in stark contrast to most gTLD Operators where there is currently no requirement to make a distinction between natural and legal persons as registrants.[37]

One of the gTLD gold standards in breaking down natural versus legal person registrations is the .NYC TLD. Under the City of New York's OpenData project, the city publishes all of the domain names registered in the TLD and the designation of the registrant as either an ORG (legal person) or INDIV (natural person).[38] According to November 2023 registration data, the majority of domains (greater than 51%) registered in the .NYC gTLD were registered to organizations. A parallel in the ccTLD community, are the annual statistics published by DNS Belgium in connection with the .BE registrant demographics.[39] In the.BE ccTLD, legal registrants (companies) currently comprise approximately 75% of the registrations, while natural persons (individuals) comprise approximately 25%.

These objective data points, coupled with anecdotal evidence regarding registration numbers associated with corporate defensive registrations and professional domain speculation (aka domainer), clearly establish that the majority of domain names are registered to legal persons (businesses) or individuals engaged in commercial activities. Unfortunately, there is little available guidance regarding domains registered in the name of individuals that are dual-use purpose (personal and commercial). Prior to the implementation of ICANN's temporary specification, .CAT had deployed a unique approach toward the disclosure of registration data associated with dual-use purpose domains. Illustrated below, is a previous

[36] See CENTR White Paper, *Registration data accuracy in European national domain registries: existing practices and challenges*. https://www.centr.org/news/news/data-accuracy-paper.html (page 10).
[37] This CircleID article co-authored by ICANN Accredited Registrar Representatives is representatives of the arguments advanced by the contracting parties against implementing a distinction between natural and legal registrants during the ICANN policy development process, see https://circleid.com/posts/20210607-privacy-legal-vs-natural-persons-and-never-ending-icann-epdp/
[38] https://data.cityofnewyork.us/Business/-nyc-Domain-Registrations/9cw8-7heb
[39] https://www.dnsbelgium.be/en/year-report-2022#number-of-be-domain-names-per-holder

approach that PuntCAT had been vetted with both ICANN and the appropriate Spanish data authorities.



Recommendations:

7.1 Member States shall require all TLD name registries and entities providing domain name registration services to tag/identify in the publicly available WHOIS/RDDS output the registrant for each registered domain as either being a natural person or a legal person.

7.2 Members States should provide guidance to TLD name registries and entities providing domain name registration services to natural persons to disclose domain registration data to third parties with a legitimate interest where the domain name is being used in commercial activity.

7.3 Member States shall require all TLD name registries and entities providing domain name registration services to operate a publicly available portal where third parties with a legitimate interest could challenge the natural/legal designation based upon the actual use of the domain.

7.4 Member States shall provide explicit guidance on dual-purpose use domains and the need to disclose registration data associated with a natural person when that domain is used in ongoing meaningful commercial activity.

8.0 Defining the Registrant to include the Beneficial Registrant

Article 23 of NIS states the database of complete and accurate domain name registration data "shall include" the registrant's name, contact email and contact telephone. However, nowhere in NIS 2.0 is registrant defined. While ICANN's Acronym and Terms database[40] defines registrant as "[a]n individual

[40] https://www.icann.org/en/icann-acronyms-and-terms

or entity who registers a domain name," it is not defined in either the 2013 ICANN Registrar Accreditation Agreement (2013 RAA)[41] or the ICANN baseline Registry Agreement[42]. The use of different terms (e.g. Holder) by some ccTLDs in their terms and conditions and their WHOIS/RDDS output further adds an element of confusion to a clear definition.

However, one of the biggest impediments to ensuring the completeness and accuracy of domain registration data is the prevalent use of proxy services in gTLDs. This is because these service providers place all domain names (sometimes hundreds of thousands or millions) registered with that provider into a single registrant account. Therefore, when a third party seeks to identify or hold the beneficial user (customer of that service) accountable for illegal activity associated with that domain name, navigating the red tape of these service providers imposes additional delay.

It appears that the drafters of NIS 2.0 attempted to account for the existence of privacy and proxy service providers by requiring "the contact email address and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant" in Article 28 Paragraph 2.d. Ideally, Members States should require that the beneficial user of any domain name registered via a privacy or proxy service provider be listed as the Admin (Administrative) Contact as designated in Specification 4 of the baseline Registry Agreement.

Recommendations:

8.1 Members States shall provide the following definition for Registrant:

Registrant means an individual or entity who registers a domain name (including a privacy or proxy service) OR is deemed the beneficial user/customer of it.

8.2 Member States shall designate privacy and proxy service providers as "entities providing domain name registration services" and require their registration under Article 27.

8.3 Members States shall require that data associated with the Registrant Organization field be publicly accessible in the database maintained by TLD name registries and entities providing domain name registration services.

8.4 Members States shall require any beneficial user (and their associated contact details) be listed as the Admin (Administrative) Contact for any domain when either a Privacy or Proxy Service Provider is listed as the Registrant (Name or Organization).

[41] Although there are multiple references to registrant(s) (lower "r") in the 2013 RAA, the only defined term in this agreement is Registered Name Holder.

[42] There are multiple references to registrant(s) (lower "r") in the baseline agreement including prominently in Specification 4 (Registration Data Publication Services), however, similar to the 2013 RAA the term in not specifically defined.

Article 21 Considerations

9.0 Domain Name Misappropriation

Article 21 of NIS 2.0 requires "essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of their networks," including supply chain security.[43] While ICANN and TLD name registries have imposed some supply chain security requirements, evidence of continued reports of domain thefts in the news and court filings suggest that domain name entities providing domain name registration services are failing to adequately safeguard these essential digital assets.

Listed below is a representative sampling of reported domain name thefts (hijackings) which calls into question the security of the entirety of the domain name supply chain.

- A resident of Portugal had to file a lawsuit alleging the misappropriation of his domain name from his Registrar's account.[44]
- The estate of Uzi Nissan filed a lawsuit alleging the theft of domain names Nissan.com and Nissan.net.[45]
- A Chinese national filed a lawsuit alleging the theft of 30 domain names from his Registrar's account.[46]
- A Japanese national filed a lawsuit alleging the theft of 9 domain names from his Registrar's account.[47]
- Two recent attacks on crypto companies involved compromised credentials at two leading registrars.[48]
- The domain name Perl.com, a repository of articles about Perl programming, news and culture, was hijacked for over a week.[49]

While a growing number of domain name registration authorities offer Multi-Factor Authentication (MFA), not all Registrars and their reseller networks providing domain name registration services offer this basic level of cybersecurity. Some Registries such as fTLD (.BANK and .INSURANCE) require MFA at both the registry AND registrar level, but most do not.[50]

The two most common attack vectors are either compromising the Registrant's credentials (most commonly obtained through a compromised email address) or compromising the Registration Authority's platform (either through social engineering or security breach). The most reported type of

[43] Article 21, Paragraph 2.d defines supply chain security as "security-related aspects concerning the relationships between each entity and its direct suppliers or service providers"
[44] https://domainnamewire.com/wp-content/brazil-domain.pdf
[45] https://domainnamewire.com/2023/06/28/estate-of-uzi-nissan-says-nissan-com-is-stolen/
[46] https://domainnamewire.com/2022/06/08/man-files-lawsuit-to-recover-30-stolen-domain-names/
[47] https://domainnamewire.com/2018/10/30/valuable-three-letter-com-domains-stolen/
[48] https://domainnamewire.com/2022/05/16/hey-crypto-companies-you-need-to-use-registry-lock/
[49] https://www.perl.com/article/the-hijacking-of-perl-com/
[50] See fTLD – https://www.ftld.com/security/

domain name misappropriation involves a criminal looking to obtain control of a domain name and then offer it for sale at a discount on the secondary market. However, a growing and perhaps more concerning trend is criminal elements looking to obtain control of the domain name to compromise the Registrant's underlying I.T. infrastructure, e.g., email, website, crypto wallets, etc. This appears to be the case in connection with some high-profile domain name hijacking incidents associated with Web 3.0 companies.[51]

Recommendations:

9.1 Member States shall require that all Registrars, Resellers and Privacy and Proxy Providers implement mandatory MFA in connection with Registrant and beneficial user access to their systems.

9.2 Members States shall require that IANA and TLD name registries implement non-phishable[52] MFA in connection with access to their systems.[53]

Article 14 Considerations – Cooperation Group

10.0 Innovation in Registrant Verification and Electronic Identification

Although a growing number of TLD name registries, both gTLD and ccTLD, have been implementing digital identity and registrant verification enhancements to their business operations, several European ccTLD Managers, in particular, are taking a thought leadership role in this area.[54] This information will be critical to the Cooperation Group's Work Stream on WHOIS as they establish guidelines to harmonize the approach to accuracy and access of registration data under Article 28. Specifically, the Task Forces on Verification and Legitimate Access are critical to establishing a baseline for the domain name ecosystem supply chain. Listed below is a current snapshot of select ccTLD name registry best practices.

The information described below was produced through a combination of methods, including a review of the policies published on the registry's websites, public presentations by ccTLD staff, and interviews with the ccTLD staff. Unfortunately, several other TLD profiles that were being researched could not be completed before this paper's publication. Recognizing the dynamic nature of this data, and the need to increase the number of TLDs surveyed, the author is contemplating several options to make this data available online in a dynamic format and to increase the number of volunteers to help curate this data.

---

[51] https://domainincite.com/30016-unstoppable-domains-goes-down-after-domain-hijack and https://siliconangle.com/2024/07/15/multiple-crypto-domains-hijacked-squarespace-due-google-domains-migration-flaw/

[52] Non-phishable MFA refers to methods that are designed to be resistant to phishing attacks by using authentication factors that are not easily intercepted or tricked, e.g. biometrics, hardware tokens, passkeys, etc.

[53] ICANN's PTI has identified "implementing passwordless authentication using new web authentication standards (e.g. passkeys)" as an FY25 Key Priority, see https://icann78.sched.com/event/1T4Kx/at-large-operations-finance-and-budget-working-group (at 47 minutes into the Zoom recording).

[54] CENTR 20th Anniversary Article, *The Role of ccTLD Managers in the Evolving Digital Identity Ecosystem*, see https://centr.org/news/news/centr-publishes-the-first-article-in-its-publication-series.html

ccTLD	Thick or Thin	Distinguish Between Natural and Legal Registrant	Proactive Scanning of Registration Data	Communication With Registrant	Notes
.DE	Thick	Yes	Yes	Current Domain Query tool provides email contact points (general & abuse) to a third party (usual registrar) to contact the registrant	The names, cities, postal codes, country codes, emails, and phones of ORG (legal person) registrants will be published to comply with NIS 2
.LT	Thick	Yes	-	The name, address, email, and telephone number of the Registrant and Technical contacts are publicly available. 3rd parties with a legitimate basis can seek access to natural person Registrant information by using the dedicated "Contact domain registrant" form provided.	The registrant is legally responsible to reply to 3rd party inquiries. Failure of the natural person Registrant to respond after 15 days is a legal basis for 3rd third party to seek access to that registration information
.BE	Thick	Yes	Yes	Currently, for legal entities, the name and address of the Registrant is publicly available, although this information is redacted for natural persons. 3rd parties can request the disclosure of the registrant's personal data, which their legal department reviews. 3rd parties can have a communication forwarded to a Registrant although they are not legally obligated to respond.	Historically, between 15-30% of all new domain name registrations are flagged for verification, with between 50% and 75% of all contact handles selected for RANT verification getting approved,
.EE	Hybrid	Yes	-	Currently, legal registrants' names and emails are published. Their telephone numbers will be published in 2025. Natural person registration data is publicly redacted by default. Third parties can use the EIF website to forward communication to the Registrant, although they are not required to respond to the inquiry.	EIF continues to retain the identity and contact details of Registrants in the registry database. EIF also offers a federated eeID service to enable reuse of verified registrants
.LV	Thick	Yes	Yes	NIC.LV currently publishes the names and addresses of legal person registrants, whereas natural person registration data is redacted. NIC.LV also operates a service by which interested 3rd parties can contact a Registrant using their web base submission form.	Natural person Registrants who are Latvian residents must also provide their Person ID number. Legal person Registrants must provide the name of the company, its registration and VAT number, and legal and postal address.

If any TLDs wish to be included in this database or wish to have certain data corrected, please contact the author by email at michael@palage.com.

10.1 .DE

DENIC is the German ccTLD manager for the .DE TLD name registry. Its 290 registrar members support over 17 million domain names registered within .DE using a traditional Registry-Registrar-Registrant model. DENIC, in consultation with its network of Registrars, identified the following principles to guide its business practices to comply with the registration data accuracy and access requirements imposed by the NIS 2.0 directive.[55]

- Future-oriented, scalable in a flexible, risk based approach;
- Mandatory check for new/updated/transferred domains;
- Check of registered domains on a complaint base;
- Ex post and ex ante verification possible; and
- Verification can be used again, even for different TLDs.

A key aspect of DENIC approach is the use of an algorithm querying the registration data[56] to undertake a Traffic-Light Risk Assessment on all domain name transactions (e.g. new registrations, updated registrations, or transfers). This risk assessment identifies a domain name registration as either low risk, suspicious, or high risk within the context of data accuracy. For domain names deemed high risk, the domain name is quarantined and withheld from the zone file until verification of the registration data can be undertaken. In the case of suspicious domain names, registrants are given a limited window to complete the verification process. If verification is not completed within the allotted time the domain name is quarantined and removed from the zone file until verification is properly completed.

DENIC does not prescribe a specific verification process for registration data. However, it does intend to publish a list of accepted verification methods and some specifics about the metadata that must be collected for these methods.[57] DENIC defers to its Registrar members to select the best verification method from this list based on its specific business model. However, Registrars are required to document and store in the metadata how the verification process took place to allow DENIC or a third party to audit this verification process at a later date. The data elements that Registrars are required to verify are: name (existence of person or organization), address (existing / not fake), and email address.

10.2 .LT

Internet Service Centre of Kaunas University of Technology d.b.a. DOMREG is the Lithuanian ccTLD manager for the .LT TLD name registry. There are currently over 120 registrars supporting over 230,000 domain names registered within .LT. Although DOMREG employs a traditional Registry-Registrar-Registrant model, Registrants can access the Registry directly to initiate a domain transfer, replacement

[55] ICANN79 ALAC Plenary Presentation https://community.icann.org/download/attachments/292978838/DENIC_Verification%5B1%5D%20%20-%20%20Read-Only.pdf?version=2&modificationDate=1709731659000&api=v2 and ROW13 Presentation https://regiops.net/sites/default/files/documents/5-ROW13-Pawel%20Kowalik-Exploring%20Synergies%20in%20NIS2%20Implementation_1.pdf

[56] DENIC operates a "thick" registry and has access to all of the registrant data in making its risk determination.

[57] This list is subject to change.

of the accredited registrar, and check the data provided by the registrar to the registry. This portal also permits the Registrant to make certain personally identifiable information (PII) associated with the domain name registration publicly available via WHOIS and also to generate a digital domain name ownership certificate.

There are no nexus requirements in connection with LT domains, DOMREG distinguishes between natural (43%) and legal person (57%) Registrants and has different protocols for how third parties can access this registration data.

For legal persons, there is no data redaction. The name, address, email and telephone of the Registrant and Technical contacts are publicly available through .LT's WHOIS service. Third parties with a legitimate basis can seek access to natural person Registrant information by querying the .LT WHOIS service and using the dedicated "Contact domain registrant" form provided. This service protects the privacy of the Registrant by forwarding the message to the Registrant, who is then legally responsible for replying within 15 days. Failure of the natural person Registrant to respond after 15 days then provides a legal basis for that third party to seek access to that registration information from DOMREG's Data Provision Portal upon paying the necessary administrative processing fee.

10.3 .BE

DNS Belgium is the Belgian ccTLD manager for the.BE TLD name registry. Approximately 1.7 million domain names are currently registered within .BE. DNS Belgium employs a traditional Registry-Registrar model in which Registrants can choose from 350 Registrars to register their name. There are currently no nexus requirements in connection with .BE domains, and DNS Belgium currently distinguishes between natural (25%) and legal (75%) person Registrants.

DNS Belgium is primarily responsible for verifying the accuracy of registrant data, although they do have a process where a Registrar can be authorized to undertake this verification. DNS Belgium employs a verification team that subjects all registrations through two review processes to identify the likelihood of a domain name being registered for abuse. The first process incorporates several algorithms to identify suspect domain names, whereas the second relies on Artificial Intelligence.[58]

The number of "hits" generated by the parameters determines whether a domain name is selected for RANT verification. If either of these processes flags a domain name as suspect, it is prevented from being delegated in zone file, and the Registrant is contacted to undergo a verification process. New registrations that are flagged for RANT verification are not delegated, only those who are not selected are delegated. Once the registrant passes the RANT verification process, their domain name is delegated. As long as the registrant does not pass (either by not reacting, either by failing the verification process) their domain stays registered in the DB but is not delegated to the zone file.

DNS Belgium operates a portal where Registrants are directed to undergo the verification process conducted by a third-party vendor. This portal offers the ability to process documents electronically, or manually upload scanned documents.

Historically, between 15-30% of all new domain name registrations are flagged for verification. Currently, DNS Belgium is at 25%. Historically, between 50% and 75% of all contact handles selected for

[58] https://www.dnsbelgium.be/en/news/predicting-domain-names-malicious-intent

RANT verification get approved, with the most recent verification pass rate for 2024 being 65%. Additional details about DNS Belgium's registrant verification process can be found on its website.[59]

DNS Belgium operates an online service where third parties can obtain registrant contact information. The output of this service identifies if a Registrant has been verified, see https://www.dnsbelgium.be/en/verification-status. For legal entities, they provide the name and address of the Registrant, although this information is redacted for natural persons. DNS Belgium also permits a third party to request the disclosure of the registrant's personal data, which their legal department reviews. Finally, DNS Belgium enables a third party to forward a communication to a Registrant (legal or natural), although the registrant is not legally obligated to respond.

10.4 .EE

The Estonian Internet Foundation (EIF) is the Estonia ccTLD manager for the.EE TLD name registry. Approximately 50 registrars support over 170,000 domain names registered within .EE.[60] Although EIF employs a traditional Registry-Registrar-Registrant model, it operates a Registrant Portal that Registrants can access using a range of digital credentials.[61] This Registrant Portal permits registrants to view all domain names for which they have been listed as the administrative contact, technical contact, private registrant, or company representative (multiple administrative contacts may be indicated for one domain name).[62] EIF's registrant portal also permits them to update their contact information.

EIF has long validated Estonian registrant information using an Estonian ID card or mobile ID. Chapter 4 of the .ee Domain Regulations sets forth the current identification and identity verification requirements to register a .EE domain.[63] These regulations require that every domain name application be electronically signed using one of the following means: an Estonia ID Card or Mobile ID; using an electronic identification tool accepted by the EIF to enable electronic signature[64]; through a separate bank transfer in the name of the Registrant; or through a verified PayPal account[65].

In 2024, EIF announced a new eeID service (electronic identification service) to authenticate users and provide them an eID that could be federated across the entire domain name supply chain ecosystem .[66] In addition to the existing authentication tools that EIF had implemented, they had partnered with Veriff to provide registrant verification services globally. This solution uses FIDO to provide passwordless

---

[59] https://www.dnsbelgium.be/en/registrant-verification and https://docs.dnsbelgium.be/be/general/registrantverification.html

[60] https://www.internet.ee/help-and-info/statistics

[61] See https://registrant.internet.ee/login. Log in to Registrant portal can be achieved by using Estonian (incl. e-residents) ID card, mobile ID, Bank link or other EU citizen's electronic ID supported by EIDAS.

[62] https://www.internet.ee/help-and-info/faq#What_is_the_registrant%E2%80%99s_portal_

[63] https://www.internet.ee/domains/ee-domain-regulation#identification-and-identity-verification-requirements

[64] The current list includes: ID card of the Republic of Finland; ID card of the Republic of Lithuania;ID card of the Kingdom of Belgium; ID card of the Republic of Latvia; and eIDAS certified Smart-ID.

[65] The Verified PayPal account option will be deprecated in 2025, see https://meedia.internet.ee/files/Explanations%20to%20.ee%20regulation%20changes%20in%20English.docx.pdf

[66] https://www.internet.ee/eeid-service, see also EIF presentation at Registration Operations Workship 13 (ROW13), Know your registrant (KYR) - making internet a safer place https://regiops.net/sites/default/files/documents/6-ROW13-Timo%20V%C3%B5hmar-Know%20your%20registrant%20%28KYR%29%20-%20making%20internet%20a%20safer%20place.pdf

authentication in compliance with the NIS cybersecurity directive; e.g., Passkey. This approach not only complies with GDPR data minimization requirements but saves on future re-verification costs associated with multiple domain names associated with the same registrant. EIF recently published a list of changes to the domain regulations to comply with NIS 2.0, these changes will go into effect on 1 February 2025.[67]

EIF operates a publicly accessible service to provide third parties access to registrant data for legitimate purposes. For legal person Registrants, the following data is published through the WHOIS service, their name, commercial registry code, and names and email addresses of their administrative and technical contacts.[68] However, beginning in February 2025, EIF will publish the telephone number of legal person Registrants to comply with NIS 2.0 requirements.[69]

For natural person Registrants, individual personal data and the data of the administrative and technical contacts (name and email) are redacted by default and are not publicly available through WHOIS. Although EIF may disclose the data of natural person registrants and their representatives to the Estonian Information System Authority (RIA) and the Estonian police for cyber security purposes. For third parties seeking access to natural person Registrant information, EIF operates a website where interested parties can compose a message and provide their contact details, which EIF will forward to the relevant Registrant. Registrants are not required to respond the inquiry which EIF forwards to them.

10.5 .LV

The Institute of Mathematics and Computer Science, University of Latvia (IMCS UL), aka NIC.LV, is the Latvian ccTLD manager for the.LV TLD name registry. Approximately 140,000 domain names are currently registered within .LV. NIC.LV employs a hybrid model that permits Registrants to register and maintain a .LV domain name directly with the Registry (61%) or through one of the 164 accredited Registrars (39%).

There are no nexus requirements in connection with .LV domains. Additionally, NIC.LV distinguishes between natural (41%) and legal (59%) person Registrants and has different protocols for how third parties can access this registration data. Natural person Registrants who are Latvian residents must also provide their Person ID number. Legal person Registrants must provide the name of the company, its registration and VAT number, and legal and postal address.

NIC.LV requires that all Registrant and contact emails are verified to be operational. In connection with legal person Registrants involving a Latvian legal entity, the Enterprise Registry of Latvia is cross-referenced to pre-populate the Registrant details. There is a daily syncing of the Enterprise Registry of Latvia data and the .LV registry to ensure the accuracy of the data and to notify the registry of business health of legal person registrants, i.e., liquidation, insolvency, or suspension of business activity. NIC.LV operates a service by which interested third parties can contact a Registrant using their web base submission form.

In connection with natural person Registrants, if the registration information looks suspicious or a third-party request challenging the accuracy is received NIC.LV has an established process to verify the Registrant information. The first step is to check bank records to see if they match the identity of the

[67] https://meedia.internet.ee/files/Explanations%20to%20.ee%20regulation%20changes%20in%20English.docx.pdf
[68] https://www.internet.ee/domains/whois-terms-and-conditions#data-published-through-the-whois-service
[69] https://meedia.internet.ee/files/Explanations%20to%20.ee%20regulation%20changes%20in%20English.docx.pdf

domain name holder or if the payment data does not contain identifiable information. The second step, is to request the Registrant to provide proof of identity

11.0 Conclusion

This inspiration for this paper was the thought leadership that European ccTLDs have undertaken to enhance accuracy and access to registrant registration data. As Member States and the Cooperation Group's Work Stream on WHOIS move forward with their respective work, they must be informed about what is possible. The Cooperator Group also needs to provide a path forward to enabling all TLD name registries and entities providing domain name registration services in the EU to meet this standard. Two fundamental principles that have driven DENIC's work in this area are worth restating: the need for reusable registrant verification credentials and a future-oriented framework. NIS 2 provides a framework for the Cooperation Group to solve problems within the domain name supply chain ecosystem that the industry has not been able to solve over the past several decades.