15 October 2018

Statement of the Non-Commercial Stakeholder Group on the Proposed gTLD-Registration Data Access Protocol (RDAP) Profile

The Non-Commercial Stakeholders Group (NCSG) welcomes the opportunity to comment on the proposed gTLD-Registration Data Access Protocol (RDAP) profile that was published for community input on 31 August 2018.[1]

The NCSG has carefully reviewed the proposed profile, and we wish to express our gratitude to all those who have contributed towards defining the profile and developing the RDAP technical implementation guide. In general, we support the proposed profile but have the following comments, concerns, and recommendations:

1) Adoption of new technology in accordance with laws and policies

The NCSG first and foremost would like to raise concern about the implementation of RDAP. Implementation of RDAP is not a compliance issue, because clearly there are many policy aspects that should be addressed by the community first before RDAP can be fully implemented. Moreover just because RDAP can technically provide some functionalities, it does not mean that contracted parties should implement those features. The community is working on these very issues that can hamper the privacy rights, expectations, and desires of domain name registrants, therefore RDAP should only be implemented through policy processes in light of data protection laws and new ICANN policies that can safeguard domain name registrant data.

This is specifically true about the ICANN org response to:

> ***"Require implementation of searchability in RDAP once an RFC provides such functionality"***
>
> *Proposal: Add a requirement in the RDAP Response Profile to require registries and registrars that are permitted and offer search capabilities, to implement (within 135 days) an RFC that supports such capabilities in RDAP.*
>
> *Rationale: Temporary Specification for gTLD Registration Data, Appendix A, section 1.2.2 requires search capabilities in RDAP for those parties that are permitted and offer such capabilities (currently in the web-based Directory Service). 2017 Base Registry Agreement, Specification 4, Section 1.10 provides requirements when offering search capabilities. At the time of this writing, search capabilities in RDAP have not been developed to match the requirements in the 2017 Base Registry Agreement. However, a requirement in the RDAP Response Profile could be added to require registries and registrars that are permitted and offer search capabilities to*

[1] https://www.icann.org/public-comments/proposed-rdap-profile-2018-08-31-en

implement (with some period for implementation, e.g., 135 days) an RFC that supports such capabilities as contractually specified."

ICANN org's suggestion here is based on the current clauses in its agreements with the contracted parties which are not congruent with existing data protection laws and which do not adequately protect the personal and sensitive information of domain name registrants.[2] The clauses in registry/registrar contracts regarding searchability must be modified to comply with the law and the future policies developed by the community. We are concerned that this push for the searchability of the personal data of domain name registrants is being sought without first a Data Protection Impact Assessment being undertaken, which may reveal significant data protection concerns within ICANN's agreements and policies that may contradict with data protection principles. We would suggest this to be the case, because in our assessment, RDAP is absent proportionate and necessary protective measures for data subjects (domain name registrants).

2) Global Applicability to protect domain name registrants data

RDAP should not only redact data where the European Union's General Data Protection Regulation is applicable. Given over 100 jurisdictions now have data protection laws, and the right to privacy is a fundamental human right, if we are providing access through RDAP then it should globally redact personal data to safeguard privacy rights.

3) Comments on the Contracted Parties' Proposal for an RDAP Technical Implementation Guide

In section 1 of this document, RDAP is defined both as *Registry Data Access Protocol* and *Registration Data Access Protocol*. We believe the correct definition is the latter, as it aligns with the title of the proposed profile and the various RDAP RFC documents, and therefore should be corrected.

In section 2.1, we understand the clause, "*The RDAP server MUST support Internationalized Domain Name (IDN) RDAP lookup queries using A-label and MAY support U-label format [RFC5890] for domain names and name server objects*" to mean it is optional for a registry or registrar to implement an RDAP directory service that supports non-ASCII IDN search strings. The NCSG believes that decision to support RDAP lookup queries and responses using both A-label and U-label should be left to policy discussion, i.e. considered through a GNSO Policy Development Process.

[2] The searchability function in Section 3.3.4 of the registrars' RAA is detrimental to data subjects privacy and is inconsistent with established data protection principles on minimizing harm and ensuring the disclosure of personal data is done so only under certain processing conditions. The same can be said for the searchability criteria in Section 1.10 Spec 4 of the Registry Base Agreement.

In section 2.2, "*An RDAP server that receives a query string with a mixture of A-labels and U-labels SHOULD reject the query,"* we support the suggestion to reject queries with a mixture of labels.

In section 3.5 the text mentions additional roles "*If the server policy supports roles which are not listed below, the server MUST provide a clear mapping of additional roles."* It is unclear to the NCSG as to what roles are being referred to here, because there is no other explanation in the appendix.

Section 6.1. reads, *"In contact entities [RFC7483], phone numbers MUST be inserted as tel properties with a voice type parameter, as specified in RFC6350, the vCard Format Specification and its corresponding JSON mapping RFC7095."*

On procedural grounds the NCSG objects to phone numbers being inserted as "MUST" properties. The Expedited Policy Development Process (EPDP) working group has not yet decided on whether or not the telephone number is a mandatory data element. We strongly suggest to re-word this section to reflect that phone numbers might not be a mandatory element in RDAP, pending the conclusion of EPDP work.

Section 1.3, RDAP servers at the moment should use TLS, the implementation plan does not require them to use TLS 1.3. TLS 1.3 which is encrypted and thwarts the middleman, should be used for these servers, namely RFC 84446. As mentioned in RFC 7525: "It is expected that the TLS 1.3 specification will resolve many of the vulnerabilities listed in this document. A system that deploys. TLS 1.3 should have fewer vulnerabilities than TLS 1.2 or below. This document is likely to be updated after TLS 1.3 gets noticeable deployment."[3]

4) Comments on the Contracted Parties' Proposal for an RDAP Response Profile

In some sections of the proposed profile, such as section 2.7.3 and section 2.7.4, policy mapping is based on the gTLD Temporary Specification, however an EPDP working group has been initiated and chartered to "determine if the Temporary Specification for gTLD Registration Data should become an ICANN Consensus Policy, as is or with some modifications while complying with the GDPR and other relevant privacy and data protection laws." The NCSG believes that in the spirit of "mapping current policy requirements to the RDAP implementation with the flexibility to incorporate future policy changes with minimal re-engineering", mention should be made of the possibility of a successor of the Temporary Specification and its appendices.

Basing its argument on the registry agreements, ICANN argues that to comply the contracted parties need to make optional fields if filled in available. NCSG disagrees. Again, this is a

[3] https://tools.ietf.org/html/rfc7525

matter of access and a policy question which must be answered before deciding whether the current contracts clauses related to this issue is valid and not against the law.

In general, some data elements that the guidelines envisage to be included in RDAP are under active discussion within the EPDP and might not be applicable in the immediate future. At one time the adoption of RDAP seemed prudent, but as we move forward with the EPDP and other community discussions, it is now clear that there are many questions that need to be answered before RDAP can be adopted by registries and registrars.

Thank you for inviting our input.