16 November 2022

Subject: SSAC2022-12: SSAC Public Comment on Proposed Amendments to the Base gTLD RA and RAA to Add RDAP Contract Obligations

Background

This correspondence provides comments from the ICANN Security and Stability Advisory Committee (SSAC) on the Proposed Amendments to the Base gTLD RA and RAA to Add RDAP Contract Obligations.[1] The SSAC wishes to thank ICANN org staff and the contracted parties for their continued work towards deploying a consistent, documented RDAP implementation for access to domain registration data as per longstanding advice from the SSAC and other community members.[2]

Per its role, the SSAC focuses on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., pertaining to the correct and reliable operation of the root zone publication system), administrative matters (e.g., pertaining to address allocation and Internet number assignment), and registration matters (e.g., pertaining to registry and registrar services). The SSAC engages in threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie and advises the ICANN community accordingly. The SSAC has no authority to regulate, enforce, or adjudicate.

SSAC Comments

Comment 1: On the topic of reporting requests for domain registration data

We note that the the following paragraph appears in the proposed agreement on page 62:[3]

> *For gTLDs that are part of a single-instance Shared Registry System,:(1) the fields whois-43-queries, web-whois-queries, searchable-whois-queries and rdap-queries in the Registry Functions Activity Report should match the sum of queries reported for the gTLDs in the single-instance Shared Registry System, and registries have the flexibility to choose how to allocate those queries across the gTLDs utilizing the single-instance Shared Registry System, and (2) the Registry Functions Activity*

[1] See Public Comment on Proposed Amendments to the Base gTLD RA and RAA to Add RDAP Contract Obligations, https://www.icann.org/en/public-comment/proceeding/proposed-amendments-to-the-base-gtld-ra-and-raa-to-add-rdap-contract-obligations-06-09-2022

[2] See SAC051: SSAC Report on WHOIS Terminology and Structure.

[3] See proposed REDLINE Base gTLD Registry Agreement, https://itp.cdn.icann.org/en/files/registry-agreement/proposed-redline-base-gtld-registry-agreement-06-09-2022-en.pdf

Report may include the total contact or host transactions for all the gTLDs in the system.

This paragraph appears to be, in-part, a response to a prior SSAC recommendation in SAC097:[4]

> *Recommendation 4: The SSAC recommends that the ICANN Board suggest to ICANN Staff to ensure that zone file access and Web-based WHOIS query statistics are accurately and publicly reported, according to well-defined standards that can be uniformly complied with by all gTLD registry operators. The Zone File Access (ZFA) metric should be clarified as soon as practicable.*

The SSAC notes that while the proposed language does attempt to address this recommendation by publishing standards, the end result may still report *per-TLD* statistics inaccurately for TLDs run under shared registry systems. This will depend upon how a shared registry operator decides to follow the guidance in the proposed language. Most worryingly, the proposed language permits an operator of multiple TLDs to allocate counts of queries to individual TLDs in an inaccurate manner, as long as the sum of all counts equals the total queries for the operator. While this is an improvement over the prior situation in some respects, in others, it potentially serves to normalize the creation of inaccurate reports, as it codifies the ability for shared registry operators to provide statistics that may not reflect the true number of queries per-TLD they operate. The SSAC concludes that this change only partially satisfies Recommendation 4 in SAC097.

Comment 2: On the topic of the sunsetting of web-based WHOIS services:

The SSAC notes that while RDAP is a web-based protocol, and will thus, by definition, provide a web-based query/response system for registration data directory services (RDDS) data, there are some potential negative ramifications of sunsetting web-based WHOIS services for end users. Such changes will depend upon individual registry and registrar deployments of their RDAP lookup services. Native RDAP output is not typically easily human-readable, which differs from the current user experience where web-based WHOIS services provide human-readable output to queries posed via registry and registrar websites. This has already been noticed by some registries and registrars who are providing both raw RDAP and formatted output for queries from their websites (e.g. CentralNIC). ICANN org has also provided a similar lookup service via a special website (https://lookup.icann.org). Some end user confusion is likely to occur if different registry and registrar operators take different approaches to providing or not providing more human-friendly outputs from their own websites for RDAP queries.

The contract amendments are silent on this issue. If this is not to be addressed via the contract amendments, it would be helpful for all contracted parties to be aware of this potential user confusion issue so that they may work to address them prior to receiving customer queries or help requests. It would also be useful for ICANN org to take this into consideration as it works on end user education materials and outreach during the transition to RDAP.

Another consideration on this topic for third parties creating their own user-friendly RDAP lookup portals is that a naive approach to providing such services could result in denial of

[4] See SAC097: SSAC Advisory Regarding the Centralized Zone Data Service (CZDS) and Registry Operator Monthly Activity Reports.

access to data due to hitting rate limits at individual registries or registrars. If such a service provides a proxied approach to lookups, it will likely trigger rate limits. Fortunately, such situations can be avoided easily due to the nature of the RDAP protocol that takes advantage of web-based methods. Such a service can provide individual clients with a formatted translation of RDAP data yet still have queries originating from the client's IP address. This would be similar to using the WHOIS service on a command line, but in contrast to WHOIS, an RDAP query can run directly in a browser. It would be useful for ICANN org to provide some guidance for people interested in creating such services with advice on how to avoid such issues along with other advice they provide for the transition to RDAP.

Rod Rasmussen
Chair, ICANN Security and Stability Advisory Committee