GNSO gTLD Registries Stakeholder Group Comments

Issue: Registration Data Access Protocol (RDAP) Operational Profile for gTLD Registries and Registrars

Date: 14 March 2016

Reference URL: https://www.icann.org/public-comments/rdap-profile-2015-12-03-en

The Registries Stakeholder Group (RySG) appreciates the opportunity to comment on the **Registration Data Access Protocol (RDAP) Operational Profile for gTLD Registries and Registrars** and wishes to offer the following comments.

We welcome the work being done by ICANN to develop a proposal for the many features of the Registration Data Access Protocol ("RDAP") that require agreement between clients and server operators to develop interoperable implementations. We are, however, concerned that the RDAP Operational Profile for gTLD Registries and Registrars" (the "Operational Profile") that has been proposed is specifically designed to produce implementations of RDAP that are intended to meet the WHOIS requirements found in the Registration Data Directory Service ("RDDS") specifications in the gTLD Registry Agreement, the 2013 Registrar Accreditation Agreement, the Additional Whois Information Policy, and the RDDS Clarification Advisory.

These documents were written to describe requirements that can be (and are being) met using the current WHOIS protocols. They do not consider the new capabilities available through features specified in RDAP, and are thus incomplete. Any RDAP implementation that is functionally equivalent to WHOIS remains functionally deficient and fundamentally flawed from a policy standpoint. Since the creation of ICANN, work to update WHOIS has been an ongoing process. Many constituencies and cross-constituency groups within ICANN have worked diligently to address the many operational issues associated with using the 33-year old WHOIS protocol to publish and access domain registration metadata.

On the policy front, ICANN formed the Expert Working Group (EWG) on gTLD Directory Services in early 2013 to "define the purpose of collecting and maintaining gTLD registration data, and consider how to safeguard the data" and to "provide a proposed model for managing gTLD directory services that addresses related data accuracy and access issues, while taking into account safeguards for protecting data." The EWG's final report, issued in June 2014, recommended that "a new approach be taken for registration data access, abandoning entirely anonymous access by everyone to everything in favor of a new paradigm that combines public access to some data with gated access to other data."

Following the EWG Final Report, the GNSO completed an Issues Report (submitted in October 2015) and has approved a motion for a Charter for the Next-Generation gTLD Registration Directory Service (RDS) to replace WHOIS (Next-Gen RDS) PDP WG. While adoption of this draft Operational Profile is premature, it should prove to be useful for the registries and registrars to consider during this policy work which is just getting underway but is a long way from being complete.

On the technology front, the Internet Engineering Task Force (IETF) published a series of RFC documents (RFCs 7480 - 7485) in March 2015 that specify RDAP, and consistent with the EWG on gTLD Directory Services' recommendation, the IETF's work on RDAP was focused on finding *new* ways to provide registration data directory services by *replacing* WHOIS. For instance, RFC 7482 describes the following significant WHOIS protocol deficiencies:

1. Lack of standardized command structures
2. Lack of standardized output and error structures
3. Lack of support for internationalization and localization
4. Lack of support for user identification, authentication and access control.

As currently specified in the IETF RFC's, RDAP addresses all of these deficiencies. The RFCs also describe a number of options for use in different operating environments, so there are many instances of decisions that need to be made by implementers to meet specific operating requirements. One specific example associated with deficiency #4 is found in the client authentication options described in RFC 7481. RDAP can be used with all of the authentication options supported by the Hypertext Transfer Protocol (HTTP), but not all of these options will work well in the domain registration operating environment. Additional specifications need to be written and additional decisions need to be made to implement and deploy a usable solution. Another specific example is that the domain status values described in RDAP do not map consistently to the domain status values defined in the Extensible Provisioning Protocol (EPP). Work needs to be done to develop a mapping of status values between the protocols to maintain consistency of interpretation.

RDAP was designed to address the WHOIS deficiencies and the EWG on gTLD Directory Services' recommendations, but as currently proposed, the Operational Profile only provides the benefits of standardized command, output and error structures (deficiencies 1 and 2 above). The proposed Operational Profile fails to address internationalization and localization of contact information (deficiency 3) and also fails to include support for RDAP's user identification, authentication and access control features (deficiency 4). As noted by the EWG, these features are needed to provide data privacy by restricting data access to appropriately authorized users. As currently written, the Operational Profile continues the practice of exposing personally identifiable information to anyone who asks.

An approach that does not include support for RDAP's internationalization and data privacy supporting features and fails to address the most significant issues with WHOIS turns unsolved WHOIS problems into unsolved RDAP problems, and our industry's history of failure to resolve WHOIS deficiencies will be repeated.

For example, Section 1.4.1 of the Operational Profile is inconsistent with the guidance given in RFC 7482 regarding processing of RDAP queries containing a mixture of IDN A-labels and U-labels. Per RFC 7482, "IDNs SHOULD NOT be represented as a mixture of A-labels and U-labels; that is, internationalized labels in an IDN SHOULD be either all A-labels or all U-labels". Section 1.4.1 of the proposed Operational Profile requires that "The RDAP server MUST support Internationalized Domain Name (IDN) RDAP lookup queries using A-label or U-label format [RFC 5890] for domain name and name server objects. The RDAP server MUST accept a mixture of the two (i.e. A-label and U-label format) in the same RDAP lookup query". This requirement is not only inconsistent with RFC 7482, it is also counter to the consensus of the IETF community regarding appropriate processing of IDN queries.

To provide another example, Section 1.4.11 of the proposed Operational Profile says that "If permitted or required by an ICANN agreement provision, waiver, or Consensus Policy, an RDAP response may contain redacted registrant, administrative, technical and/or other contact information". While this is useful in the context of providing differentiated access to data for some top-level domains that include a relatively small number of registered domains, it fails to address the data privacy issue associated with open, public access to Personally Identifiable Information (PII) associated with domain name registration. One technology that can be used to provide differentiated access in RDAP exists today and has been documented as a Standards Track Internet Draft titled "Federated Authentication for the Registration Data Access Protocol (RDAP) using OpenID Connect". What's missing are the policies associated with determining appropriate levels of access based on a user's identity and their "need to know", or stated query purpose. This gap in policy development should be addressed expeditiously and *before* the RDAP requirements are finalized to take full advantage of the capabilities available in RDAP to address internationalization, localization and privacy.

Section 3 of the Operational Profile describes implementation requirements for registrars. The requirements for registrar implementation should be consistent with the 2013 Registrar Accreditation Agreement. This implementation requirement will require registrars to commit significant resources to develop, deploy, and operate a software service that will ultimately end up being discarded when and if all gTLD registries are required to provide thick services themselves. This is not a commercially reasonable requirement.

Further to reasonable commercial considerations, with regard to 1.3.6 of the profile, which states:

> "RDAP extensions, if used, MUST be registered in the IANA's RDAP Extensions registry (https://www.iana.org/assignments/rdapextensions/rdap-extensions.xhtml), as defined in RFC7480. Deployment of RDAP extensions in gTLD Registries operated under agreement with

ICANN, are subject to approval by ICANN via the RSEP process."

If the extensions are RFC standards applicable to domain name registration services, it may be unnecessary for every registry to submit an RSEP. If an RSEP is not approved, is the registry thus in violation of its contract with ICANN, which requires adoption of the new RFCs? It is not commercially viable to submit to the RSEP process for every TLD to adopt an RFC standard that is required per the contract.

With regard to section 2.6.1., which states: "Specification 3 of the RA specifies the format and content of the monthly reporting for Registry operators. The following rows are added to the Registry Functions Activity Report under section 2:

40 rdap-queries Number of RDAP queries during the period.
41 rdap-rate-limit Number of RDAP queries refused due to rate limiting for the period.
42 rdap-redirects Number of HTTP redirects for the period. 42 rdap-authenticated Number of authenticated RDAP queries for the period.
43 rdap-search-domain Number of RDAP domain search queries for the period.
44 rdap-search-entity Number of RDAP entity search queries for the period.
45 rdap-truncatedauthorization Number of RDAP responses truncated due to authorization. Includes both results and object truncation events.
46 rdap-truncated-load Number of RDAP responses truncated due to server load. Includes both results and object truncation events.
47 rdap-truncatedunexplainable Number of RDAP responses truncated due to unexplainable reasons. Includes both results and object truncation"

These are new requirements for monthly reports, and represent a change to the Registry Agreement and thus should be negotiated with registries and not be part of an operational profile. The applicable Registry Agreements do not provide ICANN the latitude to add required outputs. For instance, according to the 2012 New gTLD RA: "ICANN may request in the future that the reports be delivered by other means and using other formats." This (and similar language in other gTLD RAs) does not provide ICANN the specific right to unilaterally require additional fields.

Appendix A of the Operational Profile notes that additional protocol specifications are needed to map Extensible Provisioning Protocol (EPP) domain status codes to RDAP status codes and extend RDAP to include events that describe the registrar expiration date (which also requires an EPP extension) and the date of the most recent database update. As of today only the domain status mappings are described in an Internet-Draft. The requirement to include these features adds a dependency on the IETF's standards development process that adds scope and schedule risk. Another significant concern with the Operational Profile is in understanding how it fits into all of the other WHOIS-related work that is currently under way. The profile fails to describe how we will ever realize a fully functional RDAP service that addresses all of the known WHOIS deficiencies, and it fails to describe how the profile relates to other WHOIS-related activities taking place in ICANN. A comprehensive, well-articulated plan that describes how all of the existing work fits into a larger strategic effort would go a long way towards mitigating the risks of contracted parties having to implement multiple incomplete solutions. This plan should be developed through a community-based process such as the Thick WHOIS Implementation Review Team that is in progress.

We are also concerned about the approach being taken to develop the profile itself[1]. The IETF has a long tradition of documenting protocol implementation profiles using the Internet-Draft and Informational RFC publication process. Here are a few recent examples:

- Adobe's RTMFP Profile for Flash Communication (RFC 7425)
- Suite B Profile for Transport Layer Security (TLS) (RFC 6460)
- Suite B Profile of Certificate Management over CMS (RFC 6403)

The registration industry used the IETF process to develop the RDAP protocol specifications. We should use the same IETF process to document an RDAP implementation profile and gain consensus for the proposals.

While it may not be feasible to expect that the implementation of RDAP should be dependent on a complete solution that addresses every shortfall or potential enhancement, the community must consider the inefficiency and unnecessary churn of a piecemeal implementation plan that is a replication of the current systems without clearly articulated benefits. There is significant risk to RDAP becoming yet another failed attempt to replace WHOIS unless there is a clear understanding of the logical sequence of steps that must be taken to address each and every WHOIS deficiency recognized by the community as a whole. As proposed, the Operational Profile does not do this.

In summary, we believe that the following things need to be done before useful, efficient implementations of RDAP can be developed and deployed to provide maximum benefit to both users and operators:

1. Policy development work should be completed before production implementations are required.
2. Needed protocol specifications (EPP status mapping, new EPP extensions, federated authentication, etc.) should be completed before production implementations are required.
3. Operators should be given the opportunity to deploy experimental pilots, prototypes, and reference implementations to inform the development of policies and production services. This will also give ICANN an opportunity to test SLA monitoring interfaces and prototypes in parallel so they can be fully supported by operators when production services are deployed.

[1] Proceeding to implementation now based on the Operational Profile creates potential contractual issues, as the obligations to implement a successor protocol to WHOIS found in the applicable Registry Agreements and in the 2013 Registrar Accreditation Agreement do not contemplate compliance with a "profile" developed by ICANN staff, but rather a "standard" developed by the IETF. Moreover, given the unfinished work, it would appear the Profile cannot be implemented on a "commercially reasonable" basis, also a contractual requirement.

4. A clear statement of direction that ties the multitude of policy efforts together should be developed and approved by the ICANN community.
5. Replacing WHOIS with RDAP now, even though it won't take advantage of key RDAP features, would likely require rework of the RA and RAA 2013 and therefore lead to the necessity of contract modifications prior to implementation of RDAP by all ROs & Registrars later after the policy and standards work is done.

Thank you for your consideration.