16 February 2016

Briefing on the Migration to RDAP

The purpose of this paper is to help inform the discussion stemming from the implementation of the Registry Data Access Protocol (RDAP), a standardized replacement for the existing WHOIS protocol, and the community actions that are the basis for the RDAP implementation. Some members of the community have identified areas of concern associated with the implementation requirements in the draft version of the RDAP Operational Profile for gTLD Registries and Registrars to be considered prior to completing the implementation work.

Overall, the RDAP profile does not establish new contractual or policy requirements, but instead serves as a roadmap connecting the newly developed replacement of the WHOIS protocol to the current contractual and policy requirements of gTLD registries and registrars.

What is RDAP?

The Registration Data Access Protocol (RDAP) is a protocol designed by the technical community in the Internet Engineering Task Force (IETF) with the intent to replace the decades-old WHOIS protocol by providing similar functionality in a modern way plus additional functionality that can be optionally turned on according to policy requirements.

The RDAP protocol provides the following benefits addressing corresponding limitations in the WHOIS protocol:

1. Internationalization support for registration data (e.g., having contact names in Chinese)
2. Standardized query, response, and error messages
3. Extensibility (e.g., easy to add output elements)
4. Secure access to data (i.e., over HTTPS that avoids eavesdropping)
5. Bootstrapping mechanism to easily find the authoritative server for a given query
6. Standardized redirection/reference mechanism (e.g., allowing a thin registry to offer a pointer to the rest of the registration information in the corresponding registrar RDAP service)
7. Builds on top of the well-known web protocol HTTP (e.g., eases implementation of the RDAP services by leveraging existing knowledge to run web services)
8. Flexibility to support various policies (e.g., differentiated access, internationalization, extensibility, etc. can be turn on/off per policy decisions)
9. Optionally enables differentiated access (e.g., to provide access to all registration data fields to only authenticated users, while the non-authenticated users only can see a subset of fields)

16 February 2016

Chronology on Replacing the WHOIS Protocol

On 19 September 2011 the ICANN's Security and Stability Advisory Committee (SSAC) issued their SAC 051 Advisory recommending that "*The ICANN community should evaluate and adopt a replacement domain name registration data access protocol.*"

On 28 October 2011, the ICANN Board passed a resolution adopting SAC 051 and directing ICANN staff to produce, in consultation with the community, a roadmap to implement SAC 051 recommendations. On 4 June 2012 ICANN published the Roadmap to implement SAC 051.

In 2012 the technical community within an IETF working group starting developing RDAP. In parallel, contractual provisions in various legacy gTLDs (.biz, .com, .info, .name, .org), the 2012 Registry Agreement (new gTLDs), and the 2013 Registrar Accreditation Agreement included the requirement to implement RDAP once standardized.

In March 2015, the work in the IETF was finalized and the RDAP Request for Comments (RFCs) were published.

In order for gTLD contracted parties to implement RDAP, a gTLD RDAP profile has to be created. The profile maps the current contractual and policy obligations for gTLD registries and registrars to RDAP features. A first draft of the gTLD RDAP profile was shared for discussion with the community in September 2015 in the gTLD-tech mailing list. An updated draft of the gTLD RDAP profile is in public comments until 18 March 2016.

In parallel to RDAP implementation efforts, ICANN is working to implement the Thick Whois policy. Particularly, part of the policy regarding common label and display requirements is within a similar implementation timeline as RDAP. Given the existence of a Policy Change Calendar intended to organize the implementation schedule and to reduce the impact in contracted parties that have to change their systems for both implementations, ICANN proposed in the ongoing public comments to synchronize timing for both the Thick Whois policy and gTLD RDAP profile. Additionally, the standardized reference mechanism that is required by the draft gTLD RDAP profile, has the potential to be used as part of the Thick Whois implementation for certain cases.

Issues raised by community members

Most of the discussions around the draft profile have been of a technical nature and are already solved or in the process of resolution. However, two issues remain that go beyond technical considerations.

Differentiated Access

On 28 November 2015, the ALAC published a Statement requesting that the profile "*must include the feature set that will support differentiated access.*" Similarly, during

and subsequent to the ICANN 54 meeting in Dublin, and in the profile public comment period, a number of parties have expressed similar requests. On the other hand, the Intellectual Property Constituency submitted a public comment stated that including a requirement for differentiated access for all gTLDs would be premature at this point given the ongoing policy work in the community.

The base Registry Agreement for new gTLDs and the 2013 Registrar Accreditation Agreement are clear in their requirements for Registration Data Directory Services (a.k.a. Whois) output: "*The fields specified below set forth the minimum output requirements*" and "*The format of responses shall contain all the elements and follow a semi-free text format outline below*", respectively. ICANN notes that the current draft gTLD RDAP profile includes language regarding differentiated access to accommodate the three legacy gTLDs that have contracts that permit such a service. The current draft RDAP profile does not create new requirements for all parties to include the feature set that will support differentiated access as this is the subject of policy development as discussed below.

Andrew Sullivan, Chair of the Internet Architecture Board (IAB) sent a proposal to the gTLD-tech mailing list. The proposal included details on how to implement differentiated access by describing two different types of access (limited access for anonymous users, and full access for authenticated users). The proposal acknowledged that the majority of current gTLD agreements and existing consensus policies do not contemplate differentiated access. The proposal suggested that differentiated access as described should be implemented by all, but not enabled until a contract change or a consensus policy on the subject had been put in place.

ICANN notes that for the three gTLDs that have differentiated access in their registry agreements, there are at least two models. The model used in .TEL and .CAT describes two levels of access. Another model used in .NAME includes four levels of access.

Additionally, there is the newly started Policy Development Process (PDP) on Registration Directory Services that has in scope the broader issue of access to registration data, including the potential for differentiated access as described in the adopted Charter for the PDP working group included in Annex C of the Final Issues Report. Given the ongoing discussions and work in the community on differentiated access, it is premature to presume a certain outcome and include a requirement for all gTLDs in the RDAP Profile. Staff has encouraged those parties interested in differentiated access to participate in the Registration Directory Services PDP.

Other members of the community have also suggested postponing the implementation of RDAP altogether until a consensus policy has been put in place by the Registration Directory Services (RDS) PDP and to then undertake a single implementation effort. In light of the foreseen benefits of RDAP described above, staff proposes to move forward with the planned implementation rather than postponing any action until the outcome

of a PDP working group on RDS, which is still in its initial phases. Indeed, it is likely to be some time before there is any consensus policy on whether differentiated access will be a required feature of any new Registration Data Directory Service (RDDS) for gTLDs, and if so the details of such a requirement.

ICANN staff takes no position regarding differentiated access. Absent a policy regarding differentiated access, the contracted parties have a requirement to implement RDAP as per their agreements. Contracted parties currently have the option to request a change to their RDDS service to allow such feature in accordance with existing policies and procedures.

Whether registrars have to implement RDAP

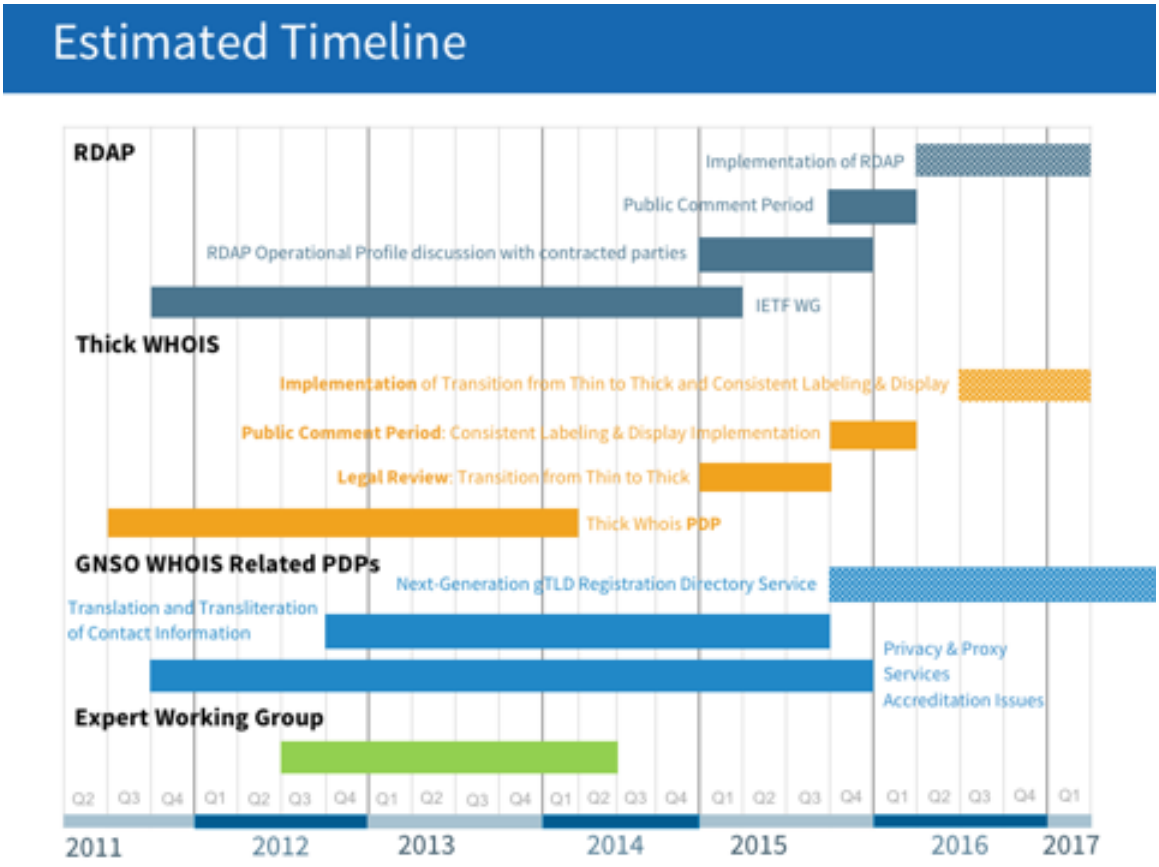
Various registrars in the gTLD-tech mailing list and the gTLD RDAP profile public comment forum have asserted that registrars should not be required to offer RDAP service for "thin registrations" (in which the registration data of the registrant, administrative, or a technical contact is not available in the registry). The comments mention that there are only three remaining thin-Whois gTLDs (.com, .jobs, and .net). Given that the Thick Whois policy implementation should transition those three to thick-Whois, the commenters state that implementation of RDAP would be of a temporary nature and is not a good use of their resources.

ICANN notes that the three thin-Whois gTLDs make for 85.6% of the registrations in the gTLD space as of October 2015[1]. The implementation of the Thick Whois policy regarding the migration of the three registries from thin to thick-Whois still has no timeline, per the Draft Thick RDDS (Whois) Consensus Policy, currently in public comment. In any case, once there is an agreed plan for this migration, it is likely to take years to be fully implemented (e.g., by doing the migration as the names come to renewal) which should facilitate implementation. Finally, there are at least two open-source RDAP server implementations[2] that registrars can use as a basis for their implementation, considerably reducing the investment they would have to make.

[1] Based on the October 2015 gTLD transaction reports publicly available at https://www.icann.org/resources/pages/reports-2014-03-04-en

[2] https://github.com/cnnic/rdap and https://github.com/RIPE-NCC/whois/tree/rdap

Annex I – Estimated Timeline of Main Whois-Related Initiatives



Annex II – Summary of RDAP Public Comments as of 31 January 2016

Dyn comments on Registration Data Access Protocol (RDAP) Operational Profile for gTLD Registries and Registrars Adam Coughlin

- The Operational Profile should require by default the ability to authenticate users from the beginning.
- It appears that the reason for registrars to need to implement RDAP is because the prevailing policy (which is being altered) requires it.
- It would be better to postpone the registrar obligation until the RDS PDP is completed; at that point, if contracted registrars are still obliged to implement RDAP, they will need to undertake only one implementation effort.

Comments from the IAB on RDAP operational profile IAB Chair

- RDAP should be deployed as soon as possible since WHOIS lacks support for authenticated access and differentiated responses.

ALAC Statement on the Registration Data Access Protocol (RDAP) Operational Profile for gTLD Registries and Registrars ICANN At-Large Staff

- While the new RDAP Operational Profile includes many new enhanced features from the previous Whois protocol, it does not include a list of mandatory features and provisions that will support an authentication access.
- While existing ICANN policies do not now require differentiated access to DNRD, it is clear from Board decisions and EWG recommendations that future ICANN policies will likely have that requirement.
- The Operational Profile of RDAP, therefore, should require differentiated now so that when differentiated access requirements are imposed, protocol features will already be deployed to provide such authentication access.

Afnic comments on RDAP Operational Profile for gTLD Registries and Registrars Régis MASSE

- We were hoping that the RDAP Profile for gTLD would include the authentication capability of the RDAP protocol since WHOIS lacks differentiated access, which will be a necessity in the future for some registries, especially in regards to data privacy.

RDAP Operational Profile for gTLD Registries and Registrars Tobias Sattler

- We would have to implement RDAP just for a few thin TLDs, while it is planned to transform these to thick gTLDs. Furthermore registrars would face additionally

effort and costs to implement RDAP that will not be required for us in the future. We would rather like to finish the transition from thin to thick first via the GNSO Thick WHOIS Policy Implementation.

JPRS Comments on "Registration Data Access Protocol (RDAP) Operational Profile for gTLD Registries and Registrars" Kentaro Mori

- Once the "thin" registries complete migration to "thick" registries, it seems that gTLD Registrars might hardly find the needs of offering RDAP services to public because all the data could be searched through gTLD Registry RDAP services.

IPC comments on RDAP operational profile Metalitz, Steven

- IPC supports ICANN's response to this, that including such a differentiated access requirement in the RDAP profile is premature.
- The PDP working group on Registry Directory Services is still in the process of formation, and it will be some time before there is any consensus policy on whether differentiated access will be a required feature of any new Registration Data Directory Service (RDDS) for gTLDs, and if so the particulars of such a requirement.
- Throughout the development of RDAP, there has been a clear distinction made between the development of a replacement technical protocol that could enable differentiated access, and the policy decision as to whether and if so under what circumstances that technical capability would be deployed.
- Confusing language over labeling required RDDS fields as OPTIONAL in the RDAP profile.
- It appears from Appendix A that the RDAP RFC's as they currently stand are not sufficient to support the RDDS policy requirements as currently defined.
- The ICANN community deserves answers to these questions before RDAP moves further ahead as a requirement for all gTLDs.