RDAP Pilot Report

25 April 2019
Version: 1.0

RDAP Pilot Background

Beginning in February 2003 with SAC003 (December 2002) and continuing through SAC027 (February 2008), SAC033 (July 2008), and finally SAC051 (September 2011), the Security and Stability Advisory Committee (SSAC) advised the ICANN community to evaluate and adopt a replacement for the existing domain name registration data access protocol, WHOIS.

In March 2015, the Internet Engineering Task Force (IETF) Web Extensible Internet Registration Data Service (WEIRDS) working group finalized the RFCs defining the Registration Data Access Protocol (RDAP), a standardized replacement for WHOIS.

On 26 July 2016, ICANN org published a gTLD Registration Data Access Protocol profile. However, the gTLD Registries Stakeholder Group requested ICANN org to not use that profile and instead work together on a modified plan to implement RDAP.

On 5 September 2017, ICANN org accepted a proposal from the gTLD Registries Stakeholder Group with support from the gTLD Registrar Stakeholder Group, and announced an RDAP pilot intended to test technical features of RDAP and build a proposal for a gTLD RDAP profile.

Starting point

One of the first decisions that the RDAP pilot group needed to make was how to go about developing a new profile. The two obvious choices were to start from scratch, or to use the staff-developed profile as a starting point. Recognizing all the work that went into the initial staff-developed profile, and not wanting to duplicate work, the pilot group agreed to use the staff-developed profile as the starting point for the development of a new RDAP profile.

In order to facilitate open discussion and collaboration, the group used Google Docs to draft the new profile. Any participant could comment, redline, or edit directly depending on their comfort level. Regular meetings were scheduled, eventually settling into a weekly cadence. Public sessions were held at each ICANN meeting starting with ICANN 60 in Abu Dhabi. An email list was created (on Google Groups) to facilitate communication and further discussion.

Policy vs. Implementation

The initial staff-developed profile contained a mix of information tied to Registration Data Directory Services (RDDS) policy requirements and purely technical RDAP implementation details. While both are needed to inform an RDAP implementation, the commingling of the two creates challenges: both policy and technology will change over time, but typically at different rates, making the maintenance of the two together difficult.

The group decided to separate the original profile into two documents: a Technical Implementation Guide, and a Response Profile.

The RDAP Technical Implementation Guide (TIG) focuses purely on the technical aspects of an RDAP server that an implementer would need to know.

The RDAP Response Profile (RP) provides a mapping to relevant RDDS policy. For registries the Registry Agreement (RA) and for registrars the Registrar Accreditation Agreement (RAA) provide base requirements for how to implement the WHOIS protocol. These requirements were later supplemented by the Additional WHOIS Information Policy (AWIP). The Consistent Labeling and Display (CL&D) policy modifies the RA and RAA changing existing requirements and adding new ones. This has been further modified by the Temporary Specification for Registration Data passed by the Board on 17 May 2018. The RDAP Response Profile attempts to distill the resultant RDDS policy requirements into instructions for use by an RDAP implementor.

GDPR Impacts

The RDAP Pilot group was originally focused on implementing legacy requirements from relevant WHOIS policies using RDAP as a substitute for WHOIS. However, the advent of the GDPR, other subsequent privacy-related policy updates from ICANN, and eventually the Temporary Specification, led to focusing efforts around how to create a Profile that fulfills policy needs while also allowing for GDPR compliance by any contracted party operating an RDAP server.

Participation Experiences and Lessons learned

Afilias

Afilias was an original advocate for the RDAP Pilot Working Group as an opportunity for the community to consider and develop the technical guidance needed for the transition to and deployment of RDAP. Afilias implemented a RDAP Server that continues to be available for the public to have access to public registration data in accordance with the 'Temporary Specification for gTLD Registration Data'. Afilias plans to implement access to non-public Registration Directory Service (RDS) data using X.509 certificates. These certificates can be used to identify, authenticate and authorize clients and consequently make access control decisions on a per-query basis. With the launching of the ePDP on Temporary Specification for gTLD Registration Data and the request from ICANN for community feedback on the Proposed Unified Access Model, we look forward to the second phase of RDAP Pilot where the community can consider and develop the technical guidance needed to support authenticated, differentiated access to non-public registration data as specified by the aforementioned policy activities.

Tucows

Tucows participated in the RDAP Pilot and appreciates the opportunity to help shape how this protocol is implemented. Tucows has already transitioned its registration data directory services to an RDAP backend, while formatting the public-facing response to appear like a Whois lookup. Tucows has also built a Tiered Access directory using RDAP, relying on the ability to filter results based on the querying user in order to comply with data protection regulations and the Specification portion of ICANN's Temporary Policy. We look forward to continuing the process of finalizing the RDAP profile and modifying our lookup results accordingly.

Verisign

Verisign has been a long-term advocate for RDAP, beginning with the co-authorship of the RDAP RFCs by Verisign's Scott Hollenbeck, and has been active in the RDAP Pilot Working Group from the beginning, with Verisign's Marc Anderson serving as its de facto chair. Verisign was one of the first Pilot Working Group participants to launch a RDAP pilot server and serviced queries throughout the Pilot. Additionally, after the publication of the Temporary Specification, Verisign modified the output of its RDAP server to comply with the Temporary Specification. During the pilot, Verisign provided data for .com, .net, and .career TLDs via its RDAP server. While the most queries were unauthenticated, Verisign successfully implemented an authenticated flow using OpenID and tested this in partnership with Viagenie. As we look forward to the next phase of the Pilot, Verisign offers these additional observations:

- The large majority of the queries received by the Verisign Pilot server were “domain lookup” queries. This means that other query paths were not vigorously exercised by clients. This is an area for future work.
- While there were successful tests of authenticated queries (using both OpenID and client-side digital certificates), these efforts did not systematically explore the full range of possibilities regarding access control. A more developed set of use cases would lead to improved testing of authentication and authorization.
- While the focus of the Pilot was on server implementations, the needs of clients (including their user interfaces and usage scenarios) is an important consideration for servers. This is also an area for future work.
- The RDAP RFCs provide for a redirect mechanism which allows a server to respond by informing the client that the answer to a query can be found elsewhere. While this redirect capability was not exercised in the current Pilot, it is an area for future work.
- Verisign exercised the RDAP bootstrap mechanism by entering its server information. However, we note that Verisign’s was the only gTLD entry placed in the bootstrap server during the pilot (others were ccTLDs) and thus we presume that the capability did not experience significant testing by clients. This is also an area for future work.

Neustar

Neustar’s RDAP service is available for all TLDs on Neustar’s platform that have opted in for the service to be active for their TLD and offers both authenticated and unauthenticated/public access. Authenticated access requires approved users to provide a Neustar issued username and password (basic auth) and a Neustar issued (closed certificate where Neustar is the CA) certificate on a per-query basis. Neustar has successfully issued access to several approved users who are actively using the service. Unauthenticated access offers reduced functionality with the most obvious being redacted data in a domain info query response. Below are a few subjects that we have worked through as part of this pilot:

- Rate limiting of unauthenticated and authenticated queries to prevent data mining and protection of PII
- Limiting “domain search queries” (e.g. domains?name=a*,domains?name=*.neustar, domains?name=*) to prevent data mining and misuse of the service
- Prevent the ability to query “entity” objects (contacts) that are not linked to a registered domain to prevent speculative searches and protection of PII

We are eagerly awaiting phase 2 of the RDAP pilot where the focus shifts to authenticated access and the method in which that is achievable and look forward to working with the community to come to a reasonable solution for users and backend operators.

CentralNic

CentralNic has been a long-term supporter of the deployment of RDAP, and participated in the standards-development process at the IETF. We are also an early-adopter of RDAP, with an implementation dating back to 2012. We also run RDAP.org, which offers a bootstrap server, web client and TLD deployment dashboard, and we've also developed a number of open source RDAP software packages, which are available on our GitLab server.

Our RDAP implementation supports use of HTTP basic authentication to provide access to non-public registration data: registrars are able to access non-public data for domains under their sponsorship; and third-parties can gain access subject to appropriate legal authorisation. Our implementation supports a flexible authentication framework, into which support for other authentication systems such as mutual TLS or OAuth2 can be integrated.

CentralNic runs a single multi-tenant, multi-TLD platform supporting both gTLDs, ccTLDs, and SLDs (such as .us.com or .radio.fm), and so its implementation has been designed to support multiple profiles, of which the gTLD RDAP Profile is only one. This approach has revealed edge cases in the ICANN profile, such as the scenario where a host object is associated with a gTLD domain but sponsored by a registrar which is not ICCAN-accredited. CentralNic was pleased to see how effectively the RDAP Pilot Working Group came to a consensus on how to resolve these issues.

Access (to registration data)

Two client identification and authentication technologies were discussed and deployed during the pilot period. The first technology uses OpenID Connect (based on OpenID and OAuth) to identify, authenticate, and authorize clients using credentials issued by a service operator known as an Identity Provider. RDAP server operators perform the role of a Relying Party in this federation. During the pilot period Verisign operated both an Identity Provider and a Relying Party, and the Verisign client supported this form of client identification and authentication for object queries in the .com, .net, and .career TLDs. Viagenie developed and operated an Identity Provider that was demonstrated to work with the Verisign Relying Party. ICANN also developed a client that was demonstrated to work with Verisign's Relying Party. This approach is documented in an Internet-Draft document:

https://datatracker.ietf.org/doc/draft-hollenbeck-regext-rdap-openid/

This service allows the Relying Party to make fine-grained authorization and access control decisions within the RDAP query service itself. Pilot implementations demonstrated that clients can be authorized based on attributes such as the purpose of their query. Attributes can be

defined on a per-query basis, or they can persist across queries as selected by an end user. Access control decisions can be made dynamically by Relying Parties on a per-query basis. This facility does not include provisions for transport-layer connection authorization.

The second technology explored during the pilot period uses digital certificates to identify and authenticate clients when they establish a TLS connection to an RDAP web service interface. The Transport Layer Security (TLS) protocol includes provisions for mutual client and server identification and authentication (see Section 7.4.6 of RFC 5246 (TLS 1.2) and Section 4.3.2 of draft-ietf-tls-tls13 (TLS 1.3)) when establishing secure HTTP (https) connection; this service leverages those capabilities. This facility allows the front-end RDAP web service to determine if a client is authorized to connect to the RDAP web service at the transport layer. It does not include provisions for query-based access control.

Certificate-based identification and authorization was implemented during the pilot period by NIC Mexico Laboratorios for domains in the (undelegated) .test TLD. DigiCert provided test certificates for client use. ICANN's client also included support for client certificates.

Although these technologies may be used individually, they are not mutually exclusive. They address different client identification, authentication, and authorization use cases. As such, they may both be useful in production systems depending on specific requirements for client access control. Phase two of the RDAP pilot will consider these issues in detail.

ICANN Staff-developed RDAP web client

In 2018, ICANN org released a prototype RDAP web client. This prototype is expected to be modified as work progresses around RDAP (e.g., the gTLD RDAP profile, the authentication choice for the accreditation model). The client runs on JavaScript; sending the query directly from the user system (e.g., user laptop accessing the client) to the RDAP server (e.g., registry or registrar). The web server does not see the query, the response, or the credentials used where the server supports authentication.

At the time of release, the client supports domain name queries to registries that have their RDAP servers listed in the IANA's "Bootstrap Service Registry for Domain Name Space" and/or the RDAP pilot. The help page provides sample domain names to query. The client supports the two authentication technologies being currently considered in the gTLD space: digital certificates, and OpenID Connect.

ICANN org Comments and Responses

On August 31, 2018, shortly before the RDAP Profile documents were posted for public comment, ICANN org provided a set of comments/issues as input to the Working Group. This input was in the context of the documents as prepared for public comment. The input consisted

of 28 specific items, each with a proposal, rationale, and a reference (if applicable), and is memorialized here: https://www.icann.org/en/system/files/files/icann-input-to-proposed-rdap-profile-31aug18-en.pdf

Quoting from the RDAP Profile public comment page (https://www.icann.org/public-comments/proposed-rdap-profile-2018-08-31-en) :

> "ICANN organization would like to clarify that it worked with a discussion group of gTLD registries and registrars to create the proposal being put for public comment. In the course of this joint effort, there emerged certain provisions for which all sides could not achieve consensus within the allotted timeline. To that end, and to maintain a reasonable implementation timeline, ICANN org has compiled its view of those differences in a separate document, which is posted along with the proposal from the discussion group of gTLD registries and registrars. ICANN org and the discussion group of gTLD registries and registrars continue their dialogue during the course of the public comment period in an effort to achieve consensus on as many of the remaining issues as possible."

Starting in September 2018 and continuing through the end of 2018, the Working Group discussed these items in its weekly meetings.

Given the relatively large number of items and their complexity, the WG tracked these in a Google spreadsheet, which was updated in real-time during meetings to track discussion and consensus.

The following table provides a summary of the Working Group consensus regarding these items. Items marked as "Agreed" were updated in the Profile documents. Note that the document section numbers referenced in the ICANN org input may not be consistent with the current document version due to document reorganization that took place during the revision process. In the table below, "TIG" refers to RDAP Technical Implementation Guide and "RP" refers to RDAP Response Profile.

Summary of Consensus Regarding ICANN org Input

Item	Summary	Reference	Consensus
1	Require the use of a TLS server certificate issued by a well-known Certificate Authority (CA)	TIG section 1.5.	Disagreed
2	Require support for RDAP domain and nameserver lookup queries in U-label format	TIG section 2.1.	Agreed
3	Require support for mixture of A-labels and U-labels in domain and nameserver lookup queries	TIG section 2.2.	Disagreed
4	Require support for JavaScript web clients	N/A	Agreed

5	Require showing data for most optional elements where data exists	RP sections 2.3.2, 2.8.4, 3.2.2, 3.3 and 4.3.	Disagreed
6	Require only one registrant, administrative, and technical contact per domain name	RP section 2.7.4.	Disagreed
7	Require a signaling mechanism for the profile version	N/A	Agreed
8	Make RDAP extensions and additional fields' requirements consistent with CL&D policy and the Temporary Specification for gTLD Registration Data	RP sections 1.1. and 1.2.	Disagreed
9	Allow contacts the possibility to opt-in to publication of full contact data (including email)	RP section 2.7.6.	Disagreed
10	Require the event "last update of RDAP database" in entity lookup responses	RP section 2.7.8	Agreed
11	Make field mappings consistent with CL&D policy	RP Appendix D.	Agreed
12	Add type to remarks element in redacted objects	RP section 2.7.5.3.	Agreed
13	Clarify requirement for registries to support registrar object lookup by name	RP, section 3.1.	Agreed
14	Clarify requirement for registries to support nameserver object lookup by IP address	RP section 2.8.2.	Agreed
15	Use RDAP features for contact email redaction requirements	RP sections 2.7.6.1 and 2.7.6.2.	Agreed
16	Add RDAP support for host objects sharing name where that is allowed in the registry system	N/A	Disagreed
17	Add optional support to include links to variant domain names	N/A	Disagreed
18	Clarify requirement for mapping of additional roles	TIG section 3.5.	Agreed
19	Require use of ISO-3166 two-letter codes instead of full country names	RP	Agreed
20	Add requirements to support LDH names in queries and responses	RP section 2.1; and TIG sections 2.1, and 4.1.	Agreed
21	Clarify that registrar and nameserver object queries only apply to registries	RP sections 3, and 4; and TIG sections 4, and 5.	Agreed
22	Clarify RFC compliance requirements	RDAP Technical Implementation Guide, sections 1.1 and 1.3.	Disagreed
23	Do not require registrars to include link to their RDAP service for a queried domain	TIG section 2.3.	Agreed
24	Omit unicodeName member in non-IDN responses	TIG section 3.1.	Disagreed

25	Require registrars to not redact contact data where a privacy/proxy service is used	RP sections 2.7.5 and 2.7.6.	Disagreed
26	Permit registries and registrars to optionally use RDAP to provide reasonable access to data per the Temporary Specification for gTLD Registration Data	RP sections 2.7.5 and 2.7.6.	Agreed
27	Require implementation of searchability in RDAP once an RFC provides such functionality	N/A	Disagreed
28	Specify what to use as handle for entity objects in thin registries	RP section 2.7.4.	Disagreed

Comments and elaboration regarding these consensus conclusions is documented here:

Item	Summary	Consensus	Comments
1	Require the use of a TLS server certificate issued by a well-known Certificate Authority (CA)	Disagreed	Extensive discussion; strong dissent registered by ICANN org. Eventual determinant centered on combination of existing practice, operational flexibility, and avoiding imposing contractual requirement
2	Require support for RDAP domain and nameserver lookup queries in U-label format	Agreed	Consensus around the support of Universal Acceptance
3	Require support for mixture of A-labels and U-labels in domain and nameserver lookup queries	Disagreed	Extensive discussion and eventual consensus that mixed labels are not sensible input from a client
4	Require support for JavaScript web clients	Agreed	Specific issue related to a requirement on RDAP servers to use the “Access-Control-Allow-Origin” header field. There was agreement that this allows for greater interoperability
5	Require showing data for most optional elements where data exists	Disagreed	Consensus was oriented around this type of requirement needing to be policy-driven. A statement requiring display of data where it exists treads toward policy and restrains the flexibility of a server operator.
6	Require only one registrant,	Disagreed	Consensus was oriented around this

	administrative, and technical contact per domain name		type of requirement needing to be policy-driven. A statement requiring display of data where it exists treads toward policy
7	Require a signaling mechanism for the profile version	Agreed	Consensus on a “two token” approach, one for the TIG and one for the RP, because these are independent docs.
8	Make RDAP extensions and additional fields' requirements consistent with CL&D policy and the Temporary Specification for gTLD Registration Data	Disagreed	Consensus that there is no reason in the Profile docs to state compliance with any particular policies because this singles out certain policies. Especially since there are statements elsewhere that the RDAP Profile isn't making policy, but is rather implementing policy Post-publication discussions at ICANN 64 (Kobe) also called into question the applicability of CL&D in the context of RDAP.
9	Allow contacts the possibility to opt-in to publication of full contact data (including email)	Disagreed	Consensus was oriented around this type of requirement needing to be policy-driven and does not belong in the RDAP Profile
10	Require the event "last update of RDAP database" in entity lookup responses	Agreed	There was some discussion of possibly changing “database” to “data source”, however, no consensus was reached on the need to change the terminology.
11	Make field mappings consistent with CL&D policy	Agreed	There was agreement that the changes identified in this issue were largely editorial
12	Add type to remarks element in redacted objects	Agreed	This change will require an update with IANA, as indicated in RFC 7483.
13	Clarify requirement for registries to support registrar object lookup by name	Agreed	To avoid expanding into searching for registrars, the solution was to map the registrar name to a handle (via URL encoding).
14	Clarify requirement for registries to support nameserver object lookup by IP address	Agreed	Lookup, in this context, is actually search, since there can be many name servers using the same IP address. The complexity of the search is limited because RFC 7882 only defines exact-match for an IP address search.

15	Use RDAP features for contact email redaction requirements	Agreed	This item triggered the need for an IETF update related to RFC 6350. See https://tools.ietf.org/html/draft-hollenbeck-vcarddav-icann-rdap-extensions for details,
16	Add RDAP support for host objects sharing name where that is allowed in the registry system	Disagreed	Disagreed on the grounds that requirements for future items should not be included in the profile. This was also considered to be a corner case.
17	Add optional support to include links to variant domain names	Disagreed	IDN variant implementations are not yet mature and have not been memorialized as consensus policy. Adding this as a requirement is approaching over-reach.
18	Clarify requirement for mapping of additional roles	Agreed	Agreed as a clarifying comment
19	Require use of ISO-3166 two-letter codes instead of full country names	Agreed	Agreement triggered work on an update to vCard documents in order to allow country codes
20	Add requirements to support LDH names in queries and responses	Agreed	Agreed as a clarifying statement
21	Clarify that registrar and nameserver object queries only apply to registries	Agreed	Agreed as a clarifying statement
22	Clarify RFC compliance requirements	Disagreed	Disagreed on the grounds that this would be a contractual requirement
23	Do not require registrars to include link to their RDAP service for a queried domain	Agreed	Agreed as a clarifying statement
24	Omit unicodeName member in non-IDN responses	Disagreed	Allowing this unicodeName member to be optional
25	Require registrars to not redact contact data where a privacy/proxy service is used	Disagreed	Disagreed on grounds that this is a policy item
26	Permit registries and registrars to optionally use RDAP to provide reasonable access to data per the Temporary Specification for gTLD Registration Data	Agreed	Agreed as a clarifying statement
27	Require implementation of searchability in RDAP once an RFC provides such	Disagreed	Disagreed on grounds on a contractual requirement, operational burden, and

	functionality		unclear future requirement.
28	Specify what to use as handle for entity objects in thin registries	Disagreed	No consensus on the applicability of the use-case.

Public Comments and Responses

The report of public comments, available here: https://www.icann.org/en/system/files/files/report-comments-proposed-rdap-profile-14dec18-en.pdf, has much of its content oriented toward community responses to the aforementioned comments from ICANN org. In those portions of the report, community input reflects agreement, disagreement, or "out of scope" related to the ICANN org input. The Working Group took this community input into account when arriving at the conclusions, documented above, related to the ICANN org input.

In addition to comments related to the ICANN org input, the Working Group also considered the input provided by the other public comments, as documented here. Some of these resulted in changes to the then-draft RDAP Profile documents and have been reflected in the versions published.

The sequencing of the comments in the below sections is different than the presentation of the comments in public comment report, however, the content is the same. This order of presentation and numbering reflects a staff-prepared working document used to facilitate Working Group discussions

For convenience, WG responses, some of which may address more than one comment, are interspersed within the comments, prefaced by an introductory label "**WG Response:**".

The following tables reflect nomenclature in the pilot comment report.

Organizations (submitting comments):

Name	**Submitted by**	**Initials**
CentralNic Group plc	Gavin Brown	CNIC
Internet Infrastructure Coalition	Monica Sanders	I2C
Registries Stakeholder Group	Samantha Demetriou	RySG
Registrars Stakeholder Group	Zoe Bonython	RrSG
At-Large Advisory Committee	ICANN Policy Staff	ALAC
Business Constituency	Steve DelBianco	BC

Non-Commercial Stakeholder Group	Rafik Dammak	NCSG
MarkMonitor	Brian J. King	MM

Individuals (submitting comments):

Name	**Affiliation (if provided)**	**Initials**
Bernhard Reutner-Fischer		BRF
Riccardo Pecile	Convey S.r.l.	RP
Mohit Batra	RSSAC caucus	MB
Mario Loffredo		MF

Issues/Recommendations from Pilot Comment Report

Extend the Pilot Program

1. The RySG "recommends an extension of the RDAP Pilot Program with the goal of conducting further testing of additional RDAP functionality such as authenticated access and the referral model, among others."

RDAP Profile documents continuous evolution

2. The RySG "expects further evolution and improvement of the RDAP Profile documents, and encourages updates to the RDAP Profile documents based on implementation experience..."
3. The RrSG explains its understanding that "this Profile is specific to the Temporary Specification adopted on 17 May 2018 and additional RDAP Profiles will need to be created in response to EPDP outcomes and/or GNSO policy development."
4. The NCSG suggests that the documents should mention the possibility of a successor of the Temporary Specification and its appendices.
5. BC notes that "several policy-related implementation changes may be pending" and expects that the "RDAP working group will be responsive with future updates to the implementation and response profiles as new policy is defined".

Global Applicability to protect domain name registrant's data

6. The NCSG suggests that RDAP "should globally redact personal data to safeguard privacy rights." (Feedback document Section 2)
7. RP suggests that the applicability of the published ICANN proposed interim model for GDPR compliance should be limited to data processing with a European Economic Area (EEA) nexus, and "compel Registrar and Registries to disclose such registrant whois personal data whenever these data would be outside the EEA."

8. BC states that "since Legal persons are not subject to GDPR, the BC believes that email addresses for Legal Persons MUST be displayed in RDAP."

WG Response: Regarding comments 1-8, the WG acknowledges these comments and either generally agrees with them (and has reflected these perspectives within the Profile documents) or had determined these items are a matter of policy and either has reflected established policy within the Profile documents or is deferring to future relevant policy developments.

Technical Comments

9. The NCSG notes that the technical document is likely to be updated to require TLS 1.3 once it gets noticeable deployment.

WG Response: The WG noted the concern and will continue to track this consideration. For this version of the documents, the WG concluded that since the documents do not refer to a specific version of TLS documents, they should require this. The WG considered adding a reference to RFC 7525, but it did not rise to a proposed change.

10. MB suggests that measures such as industry best practices and guidelines (e.g. REST Security Cheat Sheet from OWASP) and Web Application Firewalls (WAF) must be considered for the secure usage and deployment of RDAP services by ICANN and its contracted parties.

WG Response: The WG noted the concern but considered this to be beyond the scope of the Profile documents.

11. MM notes that "the vCard/jCard standard for general purpose contact information is a poor fit for domain name registration data".

WG Response: The WG noted the concern. The vCard/jCard topic was the subject of heavy discussion at various times during the WG's activities. Please see the section on this topic elsewhere in this document

12. MM also asks whether, and for how long, contracted parties should publish both WHOIS and RDAP concurrently.

WG Response: The WG determined that this topic is a policy or a contractual issue and thus is out of scope for its consideration.

13. BC notes that Whois/43 and RDAP will coexist for some time, and that there is no requirement for the caches to remain coherent between the implementations.

WG Response: The WG determined that this topic is a policy or a contractual issue and thus is out of scope for its consideration.

14. MF noted that sections 2.7.4.2, 2.7.5.1, 2.7.5.1, and 3.2.2. of the "RDAP response profile" refer incorrectly about the organization name, as well as the telephone and fax number fields as part of the "adr" jcard member, when in fact they are separate members ("org", "tel") of the jcard structure in the RDAP response. Rephrasing the wording in these sections is recommended to correctly separate the fields that belong inside the "adr" member from the fields that belong to other members.

WG Response: The WG agreed with this finding and made edits to reflect these suggestions. The WG notes that the general approach was to avoid “over specifying” the locations of the data… that is, to allow the Response Profile to focus on “what” data is needed and let existing standards express “how” that data should be conveyed.

General Suggestions

15. BRF's comment noted that in section 2.10 of the RDAP profile the required URL of the "RDDS Inaccuracy Complaint Form" is inconsistent with the required URL in section 2.6.3, and requests to revise the value by removing the "www." portion.

WG Response: The WG found that no change was required in this case as the links in question are meant to be consistent with existing practice, not necessarily consistent with each other.

16. MB's comments also state a need for 1) an analysis of the impact of the proposed RDAP profile on the rollout of the ICANN org's Privacy/Proxy Services Accreditation program, and 2) A case study regarding the deployment/usage of RDAP RFC specifications for Regional and National Internet Registries (RIRs/NIRs) in benefit of the Domain Name industry's successful implementation of the RDAP profile. Additionally, MB suggests a list of topics for preparing an FAQ document on the proposed RDAP profile, and requests that the contents of the ICANN org's URL for the RDDS Consistent Labelling and Display policy to show the latest policy version.

WG Response: While the WG found the comments to be generally interesting, they are beyond the scope of the Profile documents.

17. The ALAC expressed that the following ambiguities shall be clarified:
    - "What constitutes a ""legitimate purpose"" as it is articulated in Para. 4.4, particularly as it relates to the notion of ""accurate reliable and uniform (...) based on legitimate interests not outweigh by (...) fundamental rights"";"
    - "the framework to address appropriate law enforcement needs under Para. 4.4.9;"
    - "handling contractual compliance monitoring requests under para. 4.4.13;"

- "provisions in Annex A para. 4 that requests operators to "provide reasonable access to [data] to third parties on the basis of legitimate interests pursued by that party, except where such interest is overridden by the interests of fundamental rights and freedoms...pursuant to Article 6(1)(f) GDPR"; and
- "requirements in Appendix C, particularly ones related to outlining obligations for data registrars operating in the EU."

WG Response: While the WG found the comments to be more related to the Temporary Specification and beyond the scope of the Profile documents.

RDAP clients

18. BC suggest that RDAP Profile pertaining to RDAP clients should be defined, and "it would be beneficial for a working group to develop and share working RDAP client implementation code and test cases to ensure delivery of well-made RDAP clients in a timely fashion"

    BC notes that " The profiles as currently written seem to assume that complexity of certificate validation and internationalized domain names are best handled at the client side rather than the server side" and further elaborates that RDAP clients will be created by a multitude of parties contrary to a few contracted parties for the servers making risky in terms of compatibility and security."

WG Response: While the WG made no particular changes as a direct result of these comments, it offers general agreement with many of the ideas they contain. In particular, the WG understands the importance of clients, and has been working to consider clients when defining the server (e.g. including requirement for javascript client headers and making IDN considerations). Additionally:

- Subsequent clarifications regarding IDNs have made it clear that clients may submit U-labels to servers, thus directly addressing one of the items in the above comment.
- The WG notes that the documentation of an RDAP Profile (which is a server-side concept) should serve to drive the type of standardization that is needed for client interoperability
- The RDAP Pilot Program has included collaboration with client-side developers, including ICANN and Marc Blanchet (Viagéne)
- The WG provided a number URLs for client-side resources. This list is non-exhaustive and is not considered an endorsement by ICANN or the members of the WG, but is provided to help provide a starting point for clients.
    1. https://www.icann.org/resources/pages/rdap-information-for-users-2018-08-31-en

2. https://github.com/NICMx
3. https://github.com/arineng/nicinfo
4. https://www.openrdap.org

RDAP Profile documents should neither create nor modify existing policy

19. The RySG notes that "RDAP Profile documents should neither create nor modify existing policy, but rather be limited to mapping current policy requirements to the RDAP implementation with flexibility to incorporate future policy changes with minimal engineering".

WG Response: Being generally in agreement, the WG proposed no change related to this comment. Neither creating nor modifying policy has been a WG goal.

RDAP Profile documents partitioned between technical and policy requirements

20. The RySG support and "endorses the revised structure of the RDAP Profile documents, which essentially partitions the documentation for the RDAP Profile into elements which are policy-independent (the “RDAP Technical Implementation Guide”) and policy-dependent (the “RDAP Response Profile”). The RySG encourages the RDAP Profile to both maintain and further refine this distinction".
21. The ALAC "appreciates the RDAP's revised structure that intends to distinguish the policy independent elements and policy-dependent elements. Assuming the RDAP Profile appropriately defines such distinctions, this will ensure that ICANN removes the technical implementations of the RDAP from political considerations and debate, and, as a result, not bog down its adoption."

WG Response: Being generally in agreement, the WG proposed no change related to these comments. The WG goal in document structure has been to achieve the separation described in the above comments.

Other Important Changes

In this section, we document a small number of additional changes that occured in the Profile documents during discussions by the Working Group.

DNSSEC

The original RDAP Profile contained language that required the resource records for the RDAP service to be signed with DNSSEC. Specifically, the text said:

> "The resource records for the RDAP service MUST be signed with DNSSEC, and the DNSSEC chain of trust from the root trust anchor to the name of the RDAP server MUST be valid."

During January 2019 discussions, a participant raised the question of DNSSEC being required and proposed the normative "MUST" be changed to a "SHOULD".

In the ensuing discussion, there was general agreement about the importance of security, and the group referenced sections of the Registry Agreement related to contractual obligations around DNSSEC. The core rationale behind changing the document was that Profile documents cannot create policy or contractual requirements, which would be implied by the use of "MUST". The group reached consensus with dissent from ICANN org. This dissent was later emphasized in a message to the WG mailing list by Cyrus Namazi.

After reaching consensus, the text was changed to its published form:

> "The resource records for the RDAP service SHOULD be signed with DNSSEC, and if DNSSEC is in place, the DNSSEC chain of trust from the root trust anchor to the name of the RDAP server MUST be valid."

Registrar RDAP Service Bootstrap

During February 2019 discussions, a participant raised a question about how a Registrar's RDAP service would be located. This was in the context of the already-existing requirements related to the Registry Bootstrap Service registry, described in the TIG.

The group came to quick consensus on the technical need for a Registrar Bootstrap Service registry, however there was some discussion on the implementation approach because the Registry Bootstrap Service is documented using RFC 7484 with an IANA-supported file. The final consensus, prescribed in the Profile, was to request an update to RFC 7484 to expand IANA support to include a Registrar Bootstrap Service and to request ICANN to host an operationally compatible file at a well-known URL as a transitional solution until the RFC update is accomplished and the IANA solution is in place. Marc Blanchet, the original author of RFC 7484, subsequently volunteered to initiate an update to accomplish these changes.

The WG notes that ICANN accredited registrars MUST use the Registrar Bootstrap Service while non-accredited registrars MAY use it.

As of March 2019, the RDAP Pilot group has deferred the work on an update to RFC 7484 deciding to maintain the transitional solution indefinitely until the need arises to put effort into creating a more long-term solution.

Next Steps

At the time of document publication, the RDAP Pilot group oriented its efforts toward three concurrent tasks:

- Supporting the implementation of the February 2019 version of the ICANN gTLD RDAP Profile, which is required of ICANN accredited registries and registrars by 26 August 2019;
- Preparing for the activities of the EPDP Implementation Review Team (IRT), which are expected to result in the creation of a new RDAP Response Profile and may require changes to the RDAP Technical Implementation Guide, with deadlines presently forecasted but not finalized; and
- Tracking the progress of EPDP Phase 2, which is expected to include efforts related to authenticated and accredited disclosure of non-public registration data, with deadlines presently not forecasted.

Long Term Considerations

The most frequent long-term technical consideration expressed by members of the RDAP Pilot Working Group related to the handling of addresses and the vCard/jCard standard. As expressed by a developer from a prominent Registrar, ”It feels like we are trying to jam an old standard (vCard/jCard) into a new standard (RDAP). It doesn't follow typical api standards for building web services. If we are trying to modernize WHOIS, I am not sure this would help. Not only does it add complexity for both the consumer and web server, but I am also concerned about performance implications. Many modern json serializers are optimized for json object serialization - not for putting objects in arrays of arrays.” Another registrar provided comments that the vCard/jCard mechanism was both unintuitive and overly complicated.

Given the complexity of updating the IETF RDAP standards to use some other mechanism for handling addresses, the Working Group did not attempt an alternative approach. However, there was general agreement to continue to monitor the situation and be alert for opportunities to explore alternative solutions.