The ICANN GNSO "Business Constituency"

Comment on Proposed gTLD-Registration Data Access Protocol (RDAP) Profiles

Status: FINAL

Version: 3

13-Oct-2018

Business Constituency Submission

GNSO//CSG//BC

Background

This document is the response of the ICANN Business Constituency (BC), from the perspective of business users and registrants. As defined in our Charter, the mission of the Business Constituency is to ensure that ICANN policy positions are consistent with the development of an Internet that:

1. promotes end-user confidence because it is a safe place to conduct business
2. is competitive in the supply of registry and registrar and related services
3. is technically stable, secure and reliable.

Comment on Proposed gTLD-Registration Data Access Protocol (RDAP) Profiles[1]

In this document we respond to the request for comment on the contract parties' Proposed gTLD-Registration Data Access Protocol (RDAP) Profiles[2] and also on ICANN Org's comment on the profile[3].

First, we have several general comments on the RDAP development effort.

Need to accommodate policy changes

The BC is encouraged to see the progress made on RDAP represented by the profiles. We temper that enthusiasm by noting that several policy-related implementation changes may be pending. Although it may be impractical to "future proof" designs to anticipate future policy, it seems prudent for implementers and the profile authors to consider the open issues listed below to avoid designing ourselves into a corner.

We hope the RDAP working group will be responsive with future updates to the implementation and response profiles as new policy is defined.

Need for RDAP client profiles and prototypes

The RDAP profiles created to date are limited to RDAP servers, and there seems to be an implication that RDAP clients are now therefore also defined via inference from the server documents. Nevertheless, client implementers will benefit from corresponding Client Implementation and Request Profiles, the creation of which are likely to uncover additional areas for clarification or improvement. Similarly, 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.

Need to reduce complexity of RDAP client implementations

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. Given that RDAP clients will be created by a multitude of TBD developers, rather than the resources of the few

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

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

[3] See https://www.icann.org/en/system/files/files/icann-input-to-proposed-rdap-profile-31aug18-en.pdf

contracted parties who are defining and operating the servers, this seems a recipe for poor compatibility and security.

Need to define consistency between RDAP and Port 43 implementations
Since policy is not yet clear on how long a contracted party's Port 43 access must be maintained after an RDAP solution is delivered, we must assume that both will remain active, side by side, for some time. Under that assumption, we note that each implementation is likely to have very different connections to the underlying databases, with potentially different performance and reliability attributes, and that there is no requirement for the caches to remain coherent between the implementations.

Need the ability to federate an identity across RDAP servers
Without further development of this profile, each of the more than 1000 RDAP servers hosted by registrars and registries would require a separately issued and managed username/password. This need is explained in detail in the final section of this comment.

Need to support authorization data in future RDAP requests for non-public Whois data
BC supports the creation of an accredited access model allow access to non-public data, and ICANN Org has proposed the same concept in its Unified Access Model (UAM). To support the potential for accredited access, we should now define RDAP fields to provide credentials of the requestor and the reason for the request. This need is explained in detail in the final section of this comment.

Comment on Responses Profile offered by Contract Parties:

As a general matter, the BC believes that RDAP servers should return optional data fields when a registrant has provided data for that field. In this we agree with ICANN Org's comment #5 regarding optional data elements:

> "In order to comply with requirements in the Registry Registration Data Directory Services Consistent Labeling and Display Policy (CL&D policy), the 2017 Base Registry Agreement, and the 2013 Registrar Accreditation Agreement there should be a requirement for RDAP servers to include optional elements in the response when there is data in the registry/registrar system."

Section 2.7.5:
This BC has several concerns about this section:

- it assumes that access to registrant data under GDPR requires consent, which is not always true (as opposed to technical or admin data, perhaps)
- it assumes that consent can be collected and retrieved by the server
- it does not correspond to a defined response for returning consent data to a requestor.

Section 2.7.6
The Contract Parties Proposal said that email address MAY be given when "not subject to the GDPR" (2.7.6). Since Legal persons are not subject to GDPR, the BC believes that email addresses for Legal

Persons MUST be displayed in RDAP. Noting that the TempSpec allows redaction of email addresses not subject to GDPR, this TempSpec is for purposes of compliance and is not consensus policy.

Section 3:
vCard/jCard seems problematic since it does not currently support ISO-3166 country codes, is not supported in existing libraries for easy extraction from within a larger JSON body and does not explicitly (RFC6350 6.4.2 notwithstanding) support EAI. Support for country codes will be especially significant when evaluating applicability of local law under both existing and future policy.

Comments on ICANN input document:

Below we describe BC support and explanation for ICANN Org's comments on the Contract Parties' Proposed gTLD-Registration Data Access Protocol (RDAP) Profiles.

#1
Although the Technical Implementation Profile Section 1 includes guidance for security, and although Section 1.4 does allow support for self-signed certificates, we prefer that a requirement for a certificate from well-known CA be MUST, rather than SHOULD. Although a self-signed certificate could be implemented as per 1.4, this seems to add complication to client-side implementation, as mentioned in the general comments, above.

#2
It has been posited that there are certain use cases where it is beneficial to user experience for RDAP clients to perform U-label ⍰ A-Label conversions, allowing U-Label support on the RDAP server to be optional. After consideration, we have concluded that no such use cases exist; therefore we identify the existing profile as overly complicating client development, and support ICANN's request.

#3
We support the original profile language disallowing queries which include mixes of A-labels and U-labels and reject the ICANN suggestion. Either every label in a domain name being queried must be A-labels, or every label must be U-labels. Per Implementation Profile 3.1, queries will be returned with Unicode Name in U-Label format; even if the RDAP server persisted the mixed-format query format, there is no way to return that format during the response. Accepting one string as a query and then returning a response for a different (albeit equivalent) string could make for a bad user experience.

#4
As mentioned elsewhere, the profiles treat client development as an afterthought. This could be improved by adding a method to facilitate creation of JavaScript clients.

#5
RDAP servers should be required to return optional fields that contain data. This protects legal person registrants who benefit from data being published. This would also apply to future policies allowing the collecting and support of user consent.

#12
We support the addition of a new value. A remarks field could represent redaction distinct from truncation, could contain anonymized contact details such as a registrar-provided email alias or a link to a registrant's registrar-provided contact form.

#13
We support adding a requirement for this specific, limited form of registrar lookup by name.

#14
We support adding a requirement for this specific, limited form of nameserver lookup by IP address. If added, both IPv4 and IPv6 MUST be supported.

#20
We support adding explicit language to clarify the distinction of LDH compared to A-Labels and requirement to support both. This seems to be a recurring area of confusion for reviewers of the documents, and we should anticipate it will be a source of implementation bugs as well if not clarified.

#7, #8, #10, #11, #18, #21, #22, #23, #24, #25
We support these proposals as written.

#26
We support this comment but believe this development should include authorization credentials, as explained the final section of this document.

#9, #17, #27
See Future Policy Support, below.

#15, #19
See general vCard comments, above.

#6, #16, #28
No comment

Future RDAP Implementation Suggestions

Define RDAP fields for data that may be needed to support future ICANN policies

It is possible that we will need to define new RDAP fields to represent whether a registrant is a natural person or a legal person, and to represent whether consent to publish was given for a certain fields (i.e. registrant, technical contact, or admin contact). So we should begin now to define these fields – not the policy -- for our implementation of RDAP.

Develop the ability to federate an identity across RDAP servers

As noted in the general comment above, the BC suggests that we add the ability to federate an identity across RDAP servers. Without further development of this profile, each of the more than 1000 RDAP servers hosted by registrars and registries would require a separately issued and managed username/password.

Section 1.1.2 of the RDAP Technical Implementation Guide says that servers MUST support RFC7481 - Security Services for the Registration Data Access Protocol (RDAP). RFC7481 is given as a reference in the Contract Parties' RDAP proposal, and states:

> "RDAP's authentication framework needs to accommodate anonymous access as well as verification of identities using a range of authentication methods and credential services. To that end, RDAP clients and servers MUST implement the authentication framework specified in "Hypertext Transfer Protocol (HTTP/1.1): Authentication" [RFC7235]. The "basic" scheme can be used to send a client's user name and password to a server in plaintext, base64-encoded form. The "digest" scheme can be used to authenticate a client without exposing the client's plaintext password. If the "basic" scheme is used, HTTP over TLS [RFC2818] MUST be used to protect the client's credentials from disclosure while in transit (see Section 3.5)."

This means that servers (and clients) are ONLY required to support authentication by username and password.

Clients could be issued a certificate from a central authority and RFC7481 does say that Digital Certificates for authenticating clients can be used, but support for this feature is OPTIONAL in the RFC. Note that there are no requirements on the use of digital certificates in the RDAP Tech Implementation Guide.

RFC 7481 does discuss the use of Federated Authentication, although its support is OPTIONAL:

> The traditional client-server authentication model requires clients to maintain distinct credentials for every RDAP server. This situation can become unwieldy as the number of RDAP servers increases. Federated authentication mechanisms allow clients to use one credential to access multiple RDAP servers and reduce client credential management complexity. RDAP MAY include a federated authentication mechanism that permits a client to access multiple RDAP servers in the same federation with one credential.

The RDAP Tech Implementation Guide also does not mandate or specify the use of any federation technology. Thus clients and servers that conform to this profile will not support federation, unless we undertake this development as part of ICANN's RDAP implementation.

Support for authorization data in future RDAP requests for non-public Whois data

BC supports the creation of an accredited access model allow access to non-public data, and ICANN Org has proposed the same concept in its Unified Access Model (UAM). To support the potential for accredited access, we should now define RDAP fields to provide credentials of the requestor and the reason for the request.

Section 3.3 of RFC 7481 is given as a reference in the Contract Parties' RDAP proposal, and states:

> WHOIS does not provide services to grant different levels of access to clients based on a client's authenticated identity. As noted in Section 3.1.4.2 of "Cross Registry Internet Service Protocol (CRISP) Requirements" [RFC3707], there is utility in allowing server operators to offer "varying degrees of access depending on policy and need." Access control decisions can be made once a client's identity has been established and authenticated (see Section 3.2). Server operators MAY offer varying degrees of access depending on policy and need in conjunction with the authentication methods described in Section 3.2. If such varying degrees of access are supported, an RDAP server MUST provide granular access controls (that is, per registration data object) in order to implement authorization policies.

Support for authorization is optional (MAY) and the RDAP Tech implementation profile does not require or specify any authorization technology. Thus, clients and servers will not support any form of authorization, leaving this detail to the discretion of each of the RDAP server operators.

There is growing support for future policy where ICANN serves as a central hub for RDAP queries of non-public Whois data, when received from authenticated requestors providing a legitimate purpose for each request.

If such a service were to obtain support from ICANN community and board, and if it were legally recognized by data protection authorities, we would seriously regret not having developed the capability to provide authorization credentials and reasons as part of this RDAP implementation.

--

This Comment was drafted by Mark Svancarek, Tim Chen, Alex Deacon, Faisal Shah, Margie Milam, Stephanie Duchesneau, and Steve DelBianco.

It was approved in accord with our Charter.