ICANN org's input to the contracted parties' gTLD RDAP profile proposal

The Temporary Specification for gTLD Registration Data adopted by the ICANN Board on 17 May 2018 directed the creation of a gTLD-RDAP Profile(s), SLA, and Registry Reporting requirements as a prerequisite to launching the Registration Data Access Protocol (RDAP) service across the gTLD space. ICANN org has received a proposal from a discussion group of gTLD registries and registrars for the first item.

The proposal for a gTLD RDAP Profile consists of two documents: 1) RDAP Technical Implementation Guide; and 2) RDAP Response Profile. The former aims to provide technical instructions to gTLD registries and registrars on how to implement the RDAP service. The latter intends to map current policy requirements to the RDAP implementation with flexibility to incorporate future policy changes with minimal reengineering.

Although ICANN org provided input to the contracted parties in the development of the two documents, not all the issues raised by ICANN org have been addressed. To that end ICANN org has compiled the below input (in no particular order) to the contracted parties' proposal for gTLD RDAP profile.

1 Require the use of a TLS server certificate issued by a well-known Certificate Authority (CA)

Proposal: Update section 1.5 of the RDAP Technical Implementation Guide to say that the TLS certificate used by RDAP servers MUST (instead of SHOULD) be issued by a well-known CA, and that the CA MUST (instead of SHOULD) comply with the CAB Forum Baseline Requirements (https://cabforum.org/baseline-requirements-documents).

Rationale: To thwart a man-in-the-middle attack, an RDAP client needs, among other things, a way to validate the identity of the RDAP server. Public services that use HTTPS on the Internet are usually deployed using TLS certificates issued by a well-known CA that is trusted by the major browsers and that complies with the baseline requirements from the CA/B Forum. The language as it stands in the proposal would expose users to security risks easily avoidable with the proposed change.

Reference: RDAP Technical Implementation Guide, section 1.5.

2 Require support for RDAP domain and nameserver lookup queries in U-label format

Proposal: Update section 2.1 of the RDAP Technical Implementation Guide to say that queries in U-label forma for domain and nameserver objects MUST (instead of MAY) be supported.

Rationale: It's expected that an end-user may use his/her local language and script when querying for RDAP objects (e.g., a domain name). The RDAP client may not transform the U-labels to A-labels or may be a thin client that assembles the query from multiple sources.

An RDAP server may receive queries in U-label format when the end-user types in its local language and script, and two potential design options have been identified: 1) Require the RDAP server to process the query, or 2) Reject the query.

The robustness principle says: "Be conservative in what you send, be liberal in what you accept", therefore the design option of require the RDAP server to process the query follows the robustness principle.

Reference: RDAP Technical Implementation Guide, section 2.1.

3 Require support for mixture of A-labels and U-labels in domain and nameserver lookup queries

Proposal: Update section 2.2 of the RDAP Technical Implementation Guide to require an RDAP server to handle and respond appropriately lookup queries for domains and nameservers that mix LDH (which includes A-labels) and U-labels instead of the SHOULD requirement to reject such queries.

Rationale: It is possible for an RDAP client to assemble a query string from multiple independent data sources. Such a client might not be able to perform conversions between A-labels and U-labels. Additionally, the vast majority of users likely won't know the difference between A- and U-labels; they simply copy and paste or type the names. Requiring RDAP servers, even as a SHOULD, to reject such queries (without even specifying the rejection response) seems to be a disservice to the users.

Reference: RDAP Technical Implementation Guide, section 2.2.

4 Require support for JavaScript web clients

Proposal: Add a requirement in either the RDAP Technical Implementation Guide or the RDAP Response Profile to require RDAP servers to use the Access-Control-Allow-Origin header field.

Rationale: RFC 7480 (one of the RDAP RFCs) recommends that RDAP servers use a specific HTTP header (Cross-Origin Resource Sharing header) that enables JavaScript clients. The objective of creating JavaScript clients is to enable RDAP web clients that run in the user's system (which would enable, among other things, the existence of RDAP web clients that are able to keep the query, response and credentials out of the reach of the entity offering the web client).

Reference: N/A.

5 Require showing data for most optional elements where data exists

Proposal: Add a requirement in the RDAP Response Profile to require RDAP servers to include optional elements in the response when there is data in the registry/registrar system. For registrars, including an entity with the *reseller* role, or an event of *eventAction* type *registrar expiration* should remain as a MAY per the 2013 Registrar Accreditation Agreement.

Rationale: The documents do not have a requirement to show data for optional fields if the information exists in the SRS. For example, the 2017 Base Registry Agreement and the 2013 Registrar Accreditation Agreement require to include the "Updated Date" RDDS field in domain name query responses. The RDAP Response Profile makes including the *eventAction* type *last changed* a MAY without specifying that it MUST be provided if the domain name was updated since it was created. 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.

For registrars, including an entity with the *reseller* role, or an event of *eventAction* type *registrar expiration* should remain as a MAY per the 2013 Registrar Accreditation Agreement.

Reference: RDAP Response Profile, sections 2.3.2, 2.8.4, 3.2.2, 3.3 and 4.3.

6 Require only one registrant, administrative, and technical contact per domain name

Proposal: Modify the requirement in section 2.7.4 the RDAP Response Profile to clarify that there can only be one contact associated with a domain name for the roles: registrant, administrative contact, and technical contact.

Rationale: Section 2.7.4 the RDAP Response Profile allows for multiple entities for the roles: registrant, administrative contact, and technical contact. The 2017 Base Registry Agreement and the 2013 Registrar Accreditation Agreement only consider one contact with the aforementioned roles per domain name in the RDDS output. Similarly, the Transfer Policy considers the existence of only one registrant and one administrative contact.

Reference: RDAP Response Profile, section 2.7.4.

7 Require a signaling mechanism for the profile version

Proposal: Add a requirement in both the RDAP Technical Implementation Guide and the RDAP Response Profile to require RDAP servers to include in responses to queries the version of the gTLD RDAP profile supported.

Rationale: New versions of the profiles documents, or new profile(s) for extended functionality (i.e. authenticated responses) may be published in the future. A signaling mechanism to indicate the profiles that the response conforms to could allow an RDAP client to better parse and act on the results. For example, a *rel:related* link object has a specific semantic meaning according to the RDAP Technical Implementation Guide.

ICANN organization anticipates at least two upcoming updates to the profile documents in the short term: Translation & Transliteration policy, Uniform Access model.

Reference: RDAP Technical Implementation Guide, and RDAP Response Profile.

8 Make RDAP extensions and additional fields' requirements consistent with CL&D policy and the Temporary Specification for gTLD Registration Data

Proposal: Update the RDAP Response Profile, sections 1.1. and 1.2 to include all the requirements in section 12 of the Registry Registration Data Directory Services Consistent Labeling and Display Policy (CL&D policy) and the Temporary Specification for gTLD Registration Data.

Rationale: Section 12 of CL&D policy was mapped to the RDAP Response Profile with the exception of a few requirements. Also, a requirement on this regard in the Temporary Specification for gTLD Registration Data is missing. The following requirements would make the RDAP Response Profile consistent with section 12 of the CL&D policy and the Temporary Specification for gTLD Registration Data:

- Registrar and Registry Operator MAY output additional data fields, subject to the Data Processing requirements in Appendix C of the Temporary Specification for gTLD Registration Data.
- The RDAP extensions/additional fields MUST NOT provide confidential information of any sort.
- The RDAP extensions/additional fields MUST NOT cause a negative impact to the security, stability, or resiliency of the Internet's DNS or other systems.
- Prior to deployment, Registry Operator SHALL provide the list of all additional fields to ICANN.
- Registry Operator SHALL provide to ICANN any changes to the list of additional fields prior to deploying such changes.

It may be worth considering adding a note indicating that other policy or contractual requirements (e.g., RSEP) may apply.

Reference: RDAP Response Profile, sections 1.1. and 1.2.

9 Allow contacts the possibility to opt-in to publication of full contact data (including email)

Proposal: Update RDAP Response Profile, section 2.7.6 to allow (i.e., a MAY requirement) registries and registrars to publish the email of any contact if such contact has provided consent to do so.

Rationale: RDAP Response Profile, section 2.7.6 does not account for the possibility of contacts consenting to display their email address. Although the Temporary Specification for gTLD Registration Data does not expressly provide for it, the intent, as described in section 8 of the Calzone Model and the FAQ for implementing the Temporary Specification for gTLD Registration Data was to allow contacts the possibility to opt-in to publication of full contact data. The profile should give registries and registrars the ability to publish the full data when the contact has consented.

Reference: RDAP Response Profile, section 2.7.6.

10 Require the event "last update of RDAP database" in entity lookup responses

Proposal: Update RDAP Response Profile, section 2.7 to require including the event "last update of RDAP database" in entity lookup responses.

Rationale: Registry Agreements that support/require Whois Contact Lookup (e.g., .cat) require the inclusion of the footer "Last update of WHOIS database". In RDAP the direct equivalent is the event "last update of RDAP database". RDAP Response Profile, section 2.7 specifies the requirements for entity (contact) lookup responses; a requirement for the aforementioned event is missing.

Reference: RDAP Response Profile, section 2.7.

11 Make field mappings consistent with CL&D policy

Proposal: Update the RDDS field mappings in RDAP Response Profile, Appendix D to make them consistent with the Registry Registration Data Directory Services Consistent Labeling and Display Policy (CL&D policy). Use "RDDS" instead of "RDS" through the document, as it is used in the CL&D policy, the 2017 Base Registry Agreement and the 2013 Registrar Accreditation Agreement.

Rationale: The RDDS field names in Appendix D of the RDAP Response Profile document should be consistent with the key names in CL&D policy.

Additionally, mappings of RDDS fields from the Registry Agreement are missing or require updates in Appendix D of the RDAP Response Profile. The suggested updates are as follows:

Mapping and RDDS field name suggestions on Registrar responses:

- Mapping for the Phone Number Ext and Fax Number Ext of the Registrar and Registrar's contacts are missing.
- Mapping for "Last update of WHOIS database" is missing.
- The RDDS field "Registrar Street" should be "Street".
- The RDDS field "Registrar City" should be "City".
- The RDDS field "Registrar State/Province" should be "State/Province".
- The RDDS field "Registrar Postal Code" should be "Postal Code".
- The RDDS field "Registrar Country" should be "Country".
- The RDDS field "Registrar Phone" should be "Phone Number".
- The RDDS field "Registrar Fax" should be "Fax Number".
- The RDDS field "Registrar Email" should be "Email".
- The RDDS field "administrative/technical " Admin/Technical Contact".
- The RDDS field "Contact Phone Number" should be "Phone Number".
- The RDDS field "Contact Fax Number" should be "Fax Number".
- The RDDS field "Contact Email" should be "Email".
- The RDDS field "WHOIS Server /Referral URL" should be "Registrar WHOIS Server/Registrar URL".

Mapping and RDDS field name suggestions on Domain Name responses:

- Mapping for "Sponsoring Registrar" should be jCard "*fn*".
- Mapping for "Registrar URL" is missing.

- The RDDS field "Domain ID" should be "Registry Domain ID".
- The RDDS field "Last update of RDS Database" should be "Last update of WHOIS database".
- The RDDS field "Sponsoring Registrar" should be "Registrar".
- The RDDS field "Sponsoring Registrar IANA ID" should be "Registrar IANA ID".
- The RDDS field "Registrar RDS Server" should be "Registrar WHOIS Server".
- The RDDS field "Registrant ID" should be "Registry Registrant ID".
- The RDDS field "Registrant Phone Number" should be "Registrant Phone".
- The RDDS field "Registrant Phone Number Ext" should be "Registrant Phone Ext".
- The RDDS field "Registrant email" should be "Registrant Email".
- The RDDS field "Admin ID" should be "Registry Admin ID".
- The RDDS field "Admin Phone Number" should be "Admin Phone".
- The RDDS field "Admin Phone Number Ext" should be "Admin Phone Ext".
- The RDDS field "Admin email" should be "Admin Email".
- The RDDS field "Tech ID" should be "Registry Tech ID".
- The RDDS field "Tech Phone Number" should be "Tech Phone".
- The RDDS field "Tech Phone Number Ext" should be "Tech Phone Ext".
- The RDDS field "Tech email" should be "Tech Email".

Mapping and RDDS field name suggestions on Name Server responses:

- The RDDS field "WHOIS Server /Referral URL" should be "Registrar WHOIS Server/Registrar URL".
- The RDDS field "Last update of RDAP Database" should be "Last update of WHOIS database".

Reference: RDAP Response Profile, Appendix D.

12 Add type to remarks element in redacted objects

Proposal: Update RDAP Response Profile, section 2.7.5.3 to require that the remarks element include a type member with a value "object truncated due to authorization".

Rationale: RDAP Technical Implementation Guide, section 2.7 requires including a remarks element when truncating objects. The remarks element is required to include a type member of the appropriate type (only three are currently defined in RDAP). In redacted entity objects, RDAP Response Profile, section 2.7.5.3 already requires including a remark titled "*REDACTED FOR PRIVACY*" and a description member with a value "*Some of the data in this object has been removed.*" However, the requirement is missing the appropriate type element to flag it as such following the way RDAP works. A type "object truncated due to authorization" appears the most suitable (there are two additional types defined in RDAP: excessive load, unexplainable reasons). For clarity, in RDAP the title and the description can be defined arbitrarily, but not the type.

Reference: RDAP Response Profile, section 2.7.5.3.

13 Clarify requirement for registries to support registrar object lookup by name

Proposal: Update RDAP Response Profile, section 3.1 to require registry's RDAP servers to support registrar object search using an entity query on the *fn* element as specified in RFC 7482 section 3.2.3. Limit search to exact match (i.e., no support for wildcard characters) to mimic lookup query behavior.

Rationale: The 2017 Base Registry Agreement requires support for registrar object lookups based on the name of the registrar. Registrar object lookup by name is not currently supported by RDAP. However, RDAP supports registrar object search based on the *fn* element. Requiring registries to support registrar object search by name (*fn* element) while limiting the search to only exact match would mimic the registrar object lookup by name required by the 2017 Base Registry Agreement. Current text in the proposal requires registries to support registrar object lookup queries by name, which is not an existing feature in RDAP.

Reference: RDAP Response Profile, section 3.1.

14 Clarify requirement for registries to support nameserver object lookup by IP address

Proposal: Update RDAP Response Profile, section 2.8.2 to require registry's RDAP servers to support nameserver search queries based on IP address as defined in RFC7482 section 3.2.2. Limit search to exact match (i.e., no support for wildcard characters) to mimic lookup query behavior.

Rationale: The 2017 Base Registry Agreement requires nameserver lookup based on IP address. Nameserver object lookup by IP address is not currently supported by RDAP. However, RDAP supports nameserver search based on the *ip* element. Requiring registries to support nameserver search by IP address while limiting the search to only exact match would mimic the name server lookup by IP address required by the 2017 Base Registry Agreement. Current text in the proposal requires registries to support nameserver lookup queries by IP address, which is not an existing feature in RDAP.

Reference: RDAP Response Profile, section 2.8.2.

15 Use RDAP features for contact email redaction requirements

Proposal: Modify RDAP Response Profile, section 2.7.6.1 to require registrars to use a new vCard property (e.g., "CONTACT-URI") for the email address or link to a web form to facilitate email communication with the contact. Also, for registries, require the use of a remarks element that will include the specific string required under the Temporary Specification for gTLD Registration Data.

Rationale: The email field is being required by RDAP Response Profile, section 2.7.6.1 to contain a string that is not an email or a URL to a web page. Even though the content of the EMAIL property is free-form UTF-8 text, processors of the field will expect a standard email address and might fail with a URI or free text, as described in section 6.4.2 of RFC 6350.

This could be solved using a new vCard property to include the URI of the redirection service, which can be either email address or web page. The new property would have to be registered as described in section 10.2 of RFC 6350. Also, for registries, require the use of a remarks element that will include the specific string required under the Temporary Specification for gTLD Registration Data.

Reference: RDAP Response Profile, sections 2.7.6.1 and 2.7.6.2.

16 Add RDAP support for host objects sharing name where that is allowed in the registry system

Proposal: Add a requirement in either the RDAP Technical Implementation Guide or the RDAP Response Profile to require RDAP servers to implement (within 135 days) an RFC to support multiple host objects with the same name in RDAP. This will only apply to registries that support multiple host objects with the same name in their registration system (only a handful of them do now).

Rationale: There a few registries that support host objects with the same name in their registration system. RDAP lookup queries do not account for this. As far as we know, only a handful of gTLD registries have this feature. For these few, it would make sense to require them to support multiple host objects with the same name in RDAP once an RFC supporting this functionality is published (with some period for implementation, e.g., 135 days). In the past there was a proposal to specify this functionality. To be clear, most gTLD registries that we know of, do not support host objects with the same name in their registration system and, therefore, will not be affected by this requirement.

Reference: N/A.

17 Add optional support to include links to variant domain names

Proposal: Add a provision in either the RDAP Technical Implementation Guide or the RDAP Response Profile to recommend (a SHOULD) or at least allow (a MAY) the inclusion of a *variants* member as described in RFC 7483.

Rationale: One of the features of RDAP is support for including links to IDN variant domain names. Several gTLDs support variant domain names; adding the variant names to the RDAP output could provide valuable information to the end-user.

Reference: N/A.

18 Clarify requirement for mapping of additional roles

Proposal: Clarify language in section 3.5 of the RDAP Technical Implementation Guide to require that when using additional roles, the roles must be registered at the IANA's RDAP JSON Values registry before use.

Rationale: Section 3.5 of the RDAP Technical Implementation Guide refers to roles listed below, but no roles are defined below. Additionally, it's not clear how the mapping of additional roles is going to be provided.

Reference: RDAP Technical Implementation Guide, section 3.5.

19 Require use of ISO-3166 two-letter codes instead of full country names

Proposal: Require the use of ISO-3166 two-letter codes instead of country names in RDAP responses by adding a parameter to the vCard *ADR* property (e.g., "cc"), and requiring RDAP servers to populate it accordingly in RDAP responses. Additionally, require RDAP servers to leave the country name parameter of the *ADR* property empty.

Rationale: In WHOIS (and the related web-based Directory Service) the contractual requirements for registries and registrars in the 2017 Base Registry Agreement and the 2013 Registrar Accreditation Agreement require the use of ISO-3166 two-letter codes, not “country names”. Such a requirement helps avoid issues that would otherwise arise by having certain contentious country or territory names listed in a field called "country name".

RDAP uses jCard for entities, which is a JSON format for vCard. Section 6.3.1 of the vCard standard (RFC 6350) specifies the *ADR* structure, which includes “*the country name (full name in the language specified in Section 5.1)*”. However, the vCard standard also appears to allow for the addition of parameters as described in section 10.2 of RFC 6350.

The aforementioned issues can be avoided by having: 1) an extended parameter added to the *ADR* property (e.g., "cc" or "ISO-3166-1-alpha-2") as described in section 10.2 of RFC 6350, 2) requiring RDAP servers to populate it accordingly, and 3) requiring the country name parameter to be left empty.

Reference: RDAP Response Profile.

20 Add requirements to support LDH names in queries and responses

Proposal: Update RDAP Response Profile, section 2.1; and RDAP Technical Implementation Guide, section 4.1 to require that the *ldhName* member MUST contain the domain name/nameserver in A-label format in the case of an IDN, and the LDH name otherwise. Also, update RDAP Technical Implementation Guide, section 2.1 to require support for queries where the domain name/nameserver is LDH.

Rationale: The RDAP Response Profile, and RDAP Technical Implementation Guide appear to be missing requirements to support LDH names, which are the vast majority of the names registered in gTLDs currently. To be clear A-label is not the same as LDH; the latter is a superset of the former.

Reference: RDAP Response Profile, section 2.1; and RDAP Technical Implementation Guide, sections 2.1, and 4.1.

21 Clarify that registrar and nameserver object queries only apply to registries

Proposal: Add language to clarify that requirements in RDAP Response Profile, sections 3, and 4; and RDAP Technical Implementation Guide, sections 4, and 5 apply only to registries. Clarify that RDAP Response Profile, section 3; and RDAP Technical Implementation Guide, section 5 are about responses to registrar object queries.

Rationale: The 2017 Base Registry Agreement requires registries to support RDDS queries for: domain names, registrar objects, and nameservers. The 2013 Registrar Accreditation Agreement only requires registrars to support RDDS queries for domain names. In order to map existing RDDS requirements in RDAP it should be clarified that support for queries for registrar objects, and nameservers only apply to registries.

Additionally, RDAP Response Profile, section 3; and RDAP Technical Implementation Guide, section 5, as currently written, could be confused to be referring to queries to registrars or from registrars. It may be worth clarifying the wording to explicitly say that they are referring to registrar object queries.

Reference: RDAP Response Profile, sections 3, and 4; and RDAP Technical Implementation Guide, sections 4, and 5.

22 Clarify RFC compliance requirements

Proposal: Update RDAP Technical Implementation Guide, sections 1.1 and 1.3 to clarify that (within a certain period of time, e.g., 135 days) severs MUST be updated to support new RFC standards.

Rationale: Current language seems to allow RDAP servers to keep using old standards even when they have been obsoleted by new ones. For example, section 1.1 reads "*An RDAP server MUST implement the following RFCs **or** their respective successors*" (emphasis added).

Reference: RDAP Technical Implementation Guide, sections 1.1 and 1.3.

23 Do not require registrars to include link to their RDAP service for a queried domain

Proposal: Update RDAP Technical Implementation Guide, section 2.3 to say that the requirement to include link to the sponsoring registrar RDAP service for a given queried domain name only applies to registries.

Rationale: The requirement to include a link to the sponsoring registrar RDAP service for a given queried domain name is intended to let users know where they can find more data for the domain name. This is useful in a response from the registry, however, it adds no value in the response from the registrar. The requirement also appears confusing at least given that uses the link relation type "*related*" which, per RFC 4287 signifies that the link is related to the containing element.

Reference: RDAP Technical Implementation Guide, section 2.3.

24 Omit *unicodeName* member in non-IDN responses

Proposal: Update RDAP Technical Implementation Guide, section 3.1 to require omission of *unicodeName* member in responses to domain name queries where the domain name is not an IDN.

Rationale: Current text says that if the domain name is not an IDN, the *unicodeName* member is optional in responses to domain name queries where the domain name is not an IDN. This seems to allow inclusion of the *unicodeName* member those cases which does not make sense and could be confusing to the users and in conflict with RFC 7483.

Reference: RDAP Technical Implementation Guide, section 3.1.

25 Require registrars to not redact contact data where a privacy/proxy service is used

Proposal: Update RDAP Response Profile, sections 2.7.5 and 2.7.6 to require registrars to not redact contact data where the contact is using a privacy/proxy service.

Rationale: Per the Temporary Specification for gTLD Registration Data, Appendix A, section 2.6, registrars are required (i.e., a MUST requirement) to not redact contact data where the contact is using a privacy/proxy service. RDAP Response Profile, sections 2.7.5 and 2.7.6 do not account for that.

Reference: RDAP Response Profile, sections 2.7.5 and 2.7.6.

26 Permit registries and registrars to optionally use RDAP to provide reasonable access to data per the Temporary Specification for gTLD Registration Data

Proposal: Update RDAP Response Profile, sections 2.7.5 and 2.7.6 to allow (i.e., a MAY requirement) registries and registrars to not redact contact data on the basis of a legitimate interest pursued by the third party making the query, or relevant legal guidance as described in Temporary Specification for gTLD Registration Data, Appendix A, section 4.

Rationale: Per the Temporary Specification for gTLD Registration Data, Appendix A, section 4, registries and registrars are required to provide access to contact data on the basis of a legitimate interest pursued by the third party making the query, or relevant legal guidance. RDAP Response Profile, sections 2.7.5 and 2.7.6 do not account for that. Although, the Temporary Specification for gTLD Registration Data does not require the use of RDAP (or any other service) for this, it does not prohibit it. It would seem sensible to allow registries and registrars to use RDAP, if they so choose.

Reference: RDAP Response Profile, sections 2.7.5 and 2.7.6.

27 Require implementation of searchability in RDAP once an RFC provides such functionality

Proposal: Add a requirement in the RDAP Response Profile to require registries and registrars that are permitted and offer search capabilities, to implement (within 135 days) an RFC that supports such capabilities in RDAP.

Rationale: Temporary Specification for gTLD Registration Data, Appendix A, section 1.2.2 requires search capabilities in RDAP for those parties that are permitted and offer such capabilities (currently in the web-based Directory Service). 2017 Base Registry Agreement, Specification 4, Section 1.10 provides requirements when offering search capabilities. At the time of this writing, search capabilities in RDAP have not been developed to match the requirements in the 2017 Base Registry Agreement. However, a requirement in the RDAP Response Profile could be added to require registries and registrars that are permitted and offer search capabilities to implement (with some period for implementation, e.g., 135 days) an RFC that supports such capabilities as contractually specified.

Reference: N/A.

28 Specify what to use as handle for entity objects in thin registries

Proposal: Update RDAP Response Profile, section 2.7.4 to specify that the handle to be used for registrars for entity objects in thin registries will use a registrar-unique identifier generated by the registrar.

Rationale: RDAP Response Profile, section 2.7.4 specifies that the handle for entity objects is to use the ROID of the contact. In thin registries there is no ROID for contacts since they are not registered with the registry. Registrars should be allowed to use their own identifiers as handle for entities that are not registered with a registry.

Reference: RDAP Response Profile, section 2.7.4.

RDAP Technical Implementation Guide

31 July 2018
Version: 1.8

Contents

I. Introduction

In 2012, The Internet Engineering Task Force (IETF) chartered the WEIRDS (Web Extensible Internet Registration Data Services) working group to replace the WHOIS protocol with a RESTful data service that supports internationalization, a formal data model, and differential services. This working group concluded in early 2015 with the publication of RFC7480, RFC7481, RFC7482, RFC7483, and RFC7484 that define the Registry Data Access Protocol (RDAP) as a standardized replacement for WHOIS. RDAP supports both Regional Internet Registries (RIRs) and Domain Name Registries (DNRs). Since 2015 other RDAP internet drafts and RFCs have been created including RFC8056, draft-ietf-regext-rdap-object-tag, and draft-hollenbeck-regext-rdap-openid, and draft-lozano-rdap-nameservers-sharing-name. The global set of RDAP RFCs and Internet Drafts are referred to as the RDAP Specifications.

The purpose of this document is to provide technical instructions to Domain Name Registries and Registrars on how to implement the Registration Data Access Protocol (RDAP). This document should be used in conjunction with a RDAP Response Profile document.

II. Implementation Instruction

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1. RDAP protocol:
   - 1.1. An RDAP server MUST implement the following RFCs. Once a successor RFC is published by the IETF, it MUST be implemented ~~or their respective successors~~no later than one hundred thirty-five (135) days after ICANN gives notice.~~:~~
     - 1.1.1. RFC7480 - HTTP Usage in the Registration Data Access Protocol (RDAP)
     - 1.1.2. RFC7481 -Security Services for the Registration Data Access Protocol (RDAP)
     - 1.1.3. RFC7482 - Registration Data Access Protocol (RDAP) Query Format
     - 1.1.4. RFC7483 - JSON Responses for the Registration Data Access Protocol (RDAP)
     - 1.1.5. RFC7484 - Finding the Authoritative Registration Data (RDAP) Service
     - 1.1.6. RFC8056 - Extensible Provisioning Protocol (EPP) and Registration Data Access Protocol (RDAP) Status Mapping
   - 1.2. The RDAP service MUST be provided over HTTPS only.
   - 1.3. An RDAP server MUST use the best practices for secure use of TLS as described in RFC7525 ~~or its successors~~. Once a successor RFC is published by the IETF, it MUST be implemented no later than one hundred thirty-five (135) days after ICANN gives notice.
   - 1.4. An RDAP client SHOULD be able to successfully validate the TLS certificate used for the RDAP service with a *TLSA* record from the DNS (RFC6698 and RFC7671) published by the RDAP service provider. The certificate(s) for the RDAP service associated by DNS-Based Authentication of Named Entities (DANE) SHOULD satisfy the requirements of section 1.5.
   - 1.5. The TLS certificate used for the RDAP service ~~SHOULD~~ MUST be issued by a Certificate Authority (CA) trusted by the major browsers and mobile

Commented [A1]: Suggestion 22

Commented [A2]: Suggestion 22

Commented [A3]: Suggestion 22

Commented [A4]: Suggestion 1

operating systems such as the ones listed in the Mozilla Included CA Certificate List (https://wiki.mozilla.org/CA:IncludedCAs). The TLS certificate used for the RDAP service ~~SHOULD~~ MUST be issued by a CA that follows the latest CAB Forum Baseline Requirements (https://cabforum.org/baseline-requirements-documents).

1.6. The RDAP server MUST support both RFC7480 GET and HEAD types of HTTP methods.

1.7. An *rdapConformance* object [RFC7483] MUST be present in the topmost object of every response, and it MUST contain the conformance level of the RDAP protocol and of any extensions, as specified in RFC7483.

1.8. RDAP services MUST be available over both IPv4 and IPv6 transport.

1.9. DNSSEC Requirements:

1.9.1. 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.

1.10. RDAP servers MUST only use fully qualified domain names in RDAP responses.

1.11. Bootstrap Requirements:

1.11.1. The base URL of RDAP services MUST be registered in the IANA's Bootstrap Service registry for Domain Name Space (https://www.iana.org/assignments/rdap-dns/rdap-dns.xhtml), as described in RFC7484, through the IANA Root Zone Management system. A separate entry is required for each TLD.

1.11.2. When the RDAP service base URL needs to be changed, the previous URL and the new one MUST remain in operation until: 1) the IANA's Bootstrap Service registry for Domain Name Space is updated, and 2) the date and time in the Expires HTTP header of a HTTP/GET request performed on the IANA's Bootstrap registry for Domain Name Space (after the new URL has been published) has elapsed.

1.12. When responding to RDAP queries, RDAP servers MUST use the Access-Control-Allow-Origin header field, as specified by [W3C.REC-cors-20140116]. Unless otherwise specified, a value of "*" MUST be used.

1.13. An RDAP server that conforms to this specification MUST include the string literal "icann_rdap_technical_implementation_guide" in the "rdapConformance"

Commented [A5]: Suggestion 1

Commented [A6]: Suggestion 4

member of the topmost JSON object of all responses provided by the server. Note: "icann_rdap_technical_implementation_guide" is pending registration in the IANA RDAP Extensions Registry.

Commented [A7]: Suggestion 7

2. Responses to RDAP queries:

2.1. The RDAP server MUST support ~~Internationalized Domain Name (IDN)~~ RDAP lookup queries using ~~A-label~~LDH and ~~MAY support~~ U-label format [RFC5890] for domain names and name server objects.

Commented [A8]: Suggestion 2 and Suggestion 20

2.2. An RDAP server that receives a query string with a mixture of LDH, ~~A-labels~~ and U-labels MUST convert all the U-labels to A-labels, perform IDNA processing, and proceed with exact-match lookup~~SHOULD reject the query~~.

Commented [A9]: Suggestion 2

Commented [A10]: Suggestion 3

2.3. A registry server~~n~~'s RDAP response to a domain query MUST contain a links object as defined in [RFC7483] section 4.2., in the topmost JSON object of the response. The links object MUST contain the elements *rel:related* and *href* pointing to the Registrar's RDAP URL of the queried domain name object.

Commented [A11]: Suggestion 23

2.4. Terms of Service

2.4.1. The terms of service of the RDAP service MUST be specified in the *notices* object in the initial JSON object of the response.

2.4.2. The *notices* object MUST contain a *links* object [RFC7483] containing an URL of the RDAP service provider.

2.4.3. The RDAP service provider MUST provide a web page with the terms of service of the RDAP service at the URL contained in the links object (2.4.2) which MAY be the same as the terms or service in the notices object (2.4.1) or MAY expand upon them.

2.5. RDAP Help queries [RFC7482] MUST be answered and include a *links* member with a URL to a document that provides usage information, policy and other explanatory material.

2.6. Truncated RDAP responses MUST contain a *notices* member describing the reason for the truncation. The *notices* object type MUST be of the form “Response truncated due to {authorization|load|unexplainable reason}”.

2.7. Truncated RDAP objects MUST contain a *remarks* member describing the reason for the truncation. The *remarks* object type MUST be of the form

"Result set truncated due to {authorization|load|unexplainable reason}".

2.8. In the case where the RDAP service provider is querying its database directly, and therefore, using real-time data, the *eventAction* type *last update of RDAP database* MUST show the timestamp of the response to the query.

3. Responses to domain name RDAP queries:

3.1. If the domain name is an IDN, the top-level domain object in the RDAP response MUST contain the U-label format of the domain in the *unicodeName* member [RFC7483]. If the domain name is not an IDN, the *unicodeName* member ~~is~~ MUST NOT be included~~optional~~.

Commented [A12]: Suggestion 24

3.2. The *status* member [RFC7483] MUST be a valid status type per the IANA's RDAP JSON Values registry (https://www.iana.org/assignments/rdap-json-values/rdap-json-values.xhtml) of status type.

3.3. The *status* member of a domain object in the RDAP response MUST match the EPP status per [RFC8056] as of the updated date of the RDAP response.

3.4. *Entities* MUST use jCard [RFC7095, 3.3.1.3] structured addresses. If a street address has more than one line, it should be structured as an array of strings.

Example:

```
["adr", {}, "text",
["", "", ["123 Main Street", "Suite 3305"],
"Any Town", "CA", "91921-1234", "U.S.A."]]
```

But if it has a single line or street address, it should be structured not as an array, but as a simple string. Example:

```
["adr", {}, "text",
["", "", "123 Main Street",
"Any Town", "CA", "91921-1234", "U.S.A."]]
```

Do not structured an address like this:

```
["adr", {}, "text",
["", "", ["123 Main Street"],
"Any Town", "CA", "91921-1234", "U.S.A."]]
```

The street address should never be an array containing a single string.

3.5. If the server policy supports additional roles ~~which are not listed below~~, ~~the server MUST provide a clear mapping of additional roles~~the roles MUST be registered at the IANA's RDAP JSON Values registry before use.

Commented [A13]: Suggestion 18

3.6. If the queried domain name is allocated, the following applies: If allocated variant domain names exist for the queried domain name, or if the domain name is an allocated variant domain name, the domain object in the RDAP response SHOULD contain a *variants* member [RFC7483]. The variants *relation* member MUST contain valid variant *relation* types as defined in the IANA's RDAP JSON Values registry. If the queried domain name is an allocated variant name, the original name SHOULD be included in the *variants* member. In the case of Registrars, the *variants* member SHOULD reflect the latest known set of variant domain names and *relation* types.

Commented [A14]: Suggestion 17

4. Registry's RDAP server ~~Responses~~ responses to nameserver ~~RDAP~~ queries

Note: this section only applies to Registries.

Commented [A15]: Suggestion 21

4.1. The name server's name MUST be specified in the *ldhName* in A-label form~~at~~ for labels that are IDN labels and in LDH form otherwise.

Commented [A16]: Suggestion 20

4.2. The *unicodeName* member MAY be present in the response to a *nameserver* lookup.

4.3. In the case of a Registry in which name servers are specified as domain attributes, the existence of a name server used as an attribute for an allocated domain name MUST be treated as equivalent to the existence of a host object.

5. Registry's RDAP server ~~R~~responses to ~~R~~registrar ~~queries~~object queries

Note: this section only applies to Registries.

Commented [A17]: Suggestion 21

5.1. RDAP servers MUST support lookup for *entities* with the *registrar* role within other objects using the *handle* (as described in 3.1.5 of RFC7482). The *handle* of the *entity* with the *registrar* role MUST be equal to IANA Registrar ID. The *entity* with the *registrar* role in the RDAP response MUST contain a *publicIDs* member to identify the IANA Registrar ID from the IANA's Registrar ID registry. The type value of the *publicID* object MUST be equal to IANA Registrar ID.

6. Responses to contact RDAP queries

6.1. In contact *entities* [RFC7483], phone numbers MUST be inserted as *tel* properties with a *voice* type parameter, as specified in RFC6350, the vCard Format Specification and its corresponding JSON mapping RFC7095.

6.2. In contact *entities*, fax numbers if used, MUST be inserted as *tel* properties with a *fax* type parameter, as specified in RFC6350, the vCard Format Specification and its corresponding JSON mapping RFC7095.

Appendix A: RDAP IETF Standards

RDAP standards are a set of specifications, which together provide a complete RDAP service. Each specification is briefly described below.

RFC7480 - HTTP Usage in the Registration Data Access Protocol (RDAP)
https://tools.ietf.org/html/rfc7480
Describes usage of HTTP transport for RDAP, error messages, RDAP extensions, rate limiting and internationalization with URIs.

RFC7481 - Security Services for the Registration Data Access Protocol (RDAP)
https://tools.ietf.org/html/rfc7481
Covers access control, authentication, authorization, privacy, data confidentiality and RDAP services availability considerations.

RFC7482 - Registration Data Access Protocol (RDAP) Query Format
https://tools.ietf.org/html/rfc7482
Defines the URL patterns for networks, autonomous systems, reverse DNS, name servers, registrars and entities queries. Also covers help requests, search (wildcards) and internationalization in requests.

RFC7483 - JSON Responses for the Registration Data Access Protocol (RDAP)
https://tools.ietf.org/html/rfc7483
Defines JSON object classes for domains, name servers, entities, IP networks and autonomous system numbers. Describe answers to help queries, searches, JSON-embedded error codes and truncated answers.

RFC7484 - Finding the Authoritative Registration Data (RDAP) Service
https://tools.ietf.org/html/rfc7484
Describes a method to find the authoritative server for RDAP data.

Appendix B: Other References

RFC7485 - Inventory and Analysis of WHOIS Registration Objects
https://www.rfc-editor.org/rfc/rfc7485.txt

RFC8056 – Extensible Provisioning Protocol (EPP) and Registration Data Access Protocol (RDAP) Status Mapping
https://tools.ietf.org/html/rfc8056
Describes the mapping of the Extensible Provisioning Protocol (EPP) statuses with the statuses registered for us in the Registration Data Access Protocol (RDAP).

IANA RDAP JSON Values Registry
https://www.iana.org/assignments/rdap-json-values/rdap-json-values.xhtml
This registry defines valid values for RDAP JSON status, role, notices and remarks, event action, and domain variant relation, as defined in RFC7483.

IANA Bootstrap Service Registry for Domain Name Space
https://www.iana.org/assignments/rdap-dns/rdap-dns.xhtml

draft-lozano-rdap-nameservers-sharing-name - Nameserver objects sharing the same name, support for the Registration Data Access Protocol (RDAP)
https://tools.ietf.org/html/draft-lozano-rdap-nameservers-sharing-name
Describes a Registration Data Access Protocol (RDAP) extension that may be used to retrieve the registration information of a particular nameserver object sharing the name with other nameserver objects.

draft-ietf-regext-rdap-object-tag – Registration Data Access Protocol (RDAP) Object Tagging
https://tools.ietf.org/html/draft-ietf-regext-rdap-object-tag
Describes an update to RFC7484 by describing an operational practice that can be used to add structure to RDAP identifiers that makes it possible to identify the authoritative server for additional RDAP queries.

draft-hollenbeck-regext-rdap-openid – Federated Authentication for the Registration Data Access Protocol (RDAP) using OpenID Connect
https://tools.ietf.org/html/draft-hollenbeck-regext-rdap-openid
Describes a federated authentication system for RDAP based on OpenID Connect.

jCard: The JSON Format for vCard
https://tools.ietf.org/html/rfc7095

vCard Format Specification
https://tools.ietf.org/html/rfc6350

EPP Status Code (ICANN)
https://www.icann.org/epp

Draft Final Report from the Expert Working Group on Internationalized Registration Data
https://gnso.icann.org/en/issues/ird/ird-draft-final-10mar15-en.pdf

Study to Evaluate Available Solutions for the Submission and Display of Internationalized Contact Data
https://www.icann.org/en/system/files/files/transform-dnrd-02jun14-en.pdf

Mozilla Included CA Certificate List
https://wiki.mozilla.org/CA:IncludedCAs

RDAP Response Profile

31 July 2018
Version: 1.8

Contents

I. Introduction

In 2012, The Internet Engineering Task Force (IETF) chartered the WEIRDS (Web Extensible Internet Registration Data Services) working group to replace the WHOIS protocol with a RESTful data service that supports internationalization, a formal data model, and differential services. This working group concluded in early 2015 with the publication of RFC7480, RFC7481, RFC7482, RFC7483, and RFC7484 that define the Registry Data Access Protocol (RDAP) as a standardized replacement for WHOIS. RDAP supports both Regional Internet Registries (RIRs) and Domain Name Registries (DNRs). Since 2015 other RDAP internet drafts and RFCs have been created including RFC8056, draft-ietf-regext-rdap-object-tag, and draft-hollenbeck-regext-rdap-openid, and draft-lozano-rdap-nameservers-sharing-name. The global set of RDAP RFCs and Internet Drafts are referred to as the RDAP Specifications.

The purpose of this document is to encapsulate the operational requirements specific to Registration Data Services (RDS) in a single document which in conjunction with the RDAP Technical Implementation Guide define a domain registry RDAP implementation. This document neither creates nor modifies existing policy, rather it maps current policy requirements to the RDAP implementation with flexibility to incorporate future policy changes with minimal reengineering.

II. Policy Mapping

This document specifies the RDAP Policy requirements from the ICANN Temporary Specification for gTLD Registration Data (the “Temporary Specification”) effective 25 May 2018 which builds upon the existing legacy Whois requirements. The following source material forms the basis for the policy mapping used to create the RDAP Response Profile.

gTLD Base Registry Agreement (RA):
https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf

2013 Registrar Accreditation Agreement
https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

Additional Whois Information Policy (AWIP),
https://www.icann.org/resources/pages/policy-awip-2014-07-02-en

Registry Registration Data Directory Services Consistent Labeling and Display Policy (CL&D),
https://www.icann.org/resources/pages/rdds-labeling-policy-2017-02-01-en

Temporary Specification for gTLD Registration Data –
https://www.icann.org/en/system/files/files/gtld-registration-data-temp-spec-17may18-en.pdf

III. Access Requirements

The RDAP implementation based on ICANN's Temporary Specification assumes multiple layers of access to RDS data. A basic, public layer provides access to some data, restricting access to most personal data, while one or more additional layers, available via future accreditation program allows access to additional elements from the registration data set.

Data from the registration data set can optionally be provided in the public layer provided that certain conditions are met (e.g., a registrant consents to full publication, or the registrant is not in the European Economic Area and the registrar optionally publishes additional data).

IV. Display Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

RDDS fields, RDAP events and RDAP elements indicated as "Optional" in this document are REQUIRED to be included in a response when data exists in the Registry or Registrar database.

Commented [A1]: Suggestion 5

1. General

1.1. These requirements represent the minimum baseline for RDAP query responses. RDAP server operators MAY output additional RDDS fields, RDAP *events* or RDAP *roles* without further approval by ICANN except as restricted below.

Commented [A2]: Suggestion 8

1.2. RDAP extensions

1.2.1. RDAP extensions, if used, MUST be registered in the IANA's RDAP Extensions registry (https://www.iana.org/assignments/rdap-extensions/rdap-extensions.xhtml), as defined in RFC7480.

1.2.2. RDAP extensions MUST NOT add browser executable code (e.g., Javascript) to the response.

1.3. The contracted parties MAY output additional data fields, subject to the Data Processing requirements in Appendix C of the Temporary Specification for gTLD Registration Data.

1.4. The RDAP extensions / additional fields MUST NOT provide confidential information of any sort, nor cause a negative impact to the security, stability, or resiliency of the Internet's DNS or other systems.

1.5. Prior to deployment, registry SHALL provide the list of all additional fields to ICANN.

1.6. Registry SHALL provide to ICANN any changes to the list of additional fields prior to deploying such changes.

Commented [A3]: Suggestion 8

1.7. An RDAP server that conforms to this specification MUST include the string literal "icann_rdap_response_profile" in the "rdapConformance" member of the topmost JSON object of all responses provided by the server. Note: "icann_rdap_response_profile" is pending registration in the IANA RDAP Extensions Registry.

Commented [A4]: Suggestion 7

1.8. ISO 3166-1 alpha 2

1.8.1. The country name parameter of the adr structure entity object MUST be empty.

1.8.2. Entities in RDAP responses MUST use the *ISO-3166-1-alpha-2* property. Note: *ISO-3166-1-alpha-2* is pending registration in the IANA vCard Elements Registry.

Commented [A5]: Suggestion 19

1.9. Registries and registrars that are permitted and offer search capabilities MUST implement the search capabilities in RDAP matching the requirement in their respective agreements and/or consensus policies, no later than one hundred thirty-five (135) days after ICANN gives notice that an RFC defining these capabilities has been published.

Commented [A6]: Suggestion 27

2. Responses to Domain name RDAP queries

2.1. Domain Name - The top-level domain object [RFC7483] in the RDAP response MUST contain the domain name in the ldhName member [RFC7483]. In the case of IDN labels, the A-label format [RFC5890] MUST be used ~~of the domain in the *ldhName* member [RFC7483]~~.

Commented [A7]: Suggestion 20

2.2. Registry Domain ID - The *domain* object *handle* in the RDAP response MUST contain the Repository Object Identifier (ROID of the domain object, <*domain:roid*> as defined in RFC5731) for the domain name object.

2.3. Event Actions (Updated, Creation, Registry Expiry, Registrar Registration Expiration, Transfer dates)

2.3.1. The domain object in the RDAP response MUST contain the following events:

2.3.1.1. Event of *eventAction* type *registration*

2.3.1.2. Event of *eventAction* type *expiration*

2.3.1.3. Event of *eventAction* type *last update of RDAP database* with a value equal to the timestamp when the RDAP database was last updated

2.3.2. The domain object in the RDAP response MAY contain the following Optional events:

2.3.2.1. An event of *eventAction* type *registrar expiration*.

2.3.2.2. Event of *eventAction* type *last changed* - The event of *eventAction* type *last changed* MUST be omitted if the domain name has not been updated since it was created

2.3.2.3. An event of *eventAction* type *transfer*, with the last date and time that the domain was transferred. The event of *eventAction* type *transfer* MUST be omitted if the domain name has not been transferred since it was created.

2.4. Registrar (Registrar Entity)

2.4.1. Registrar - The *domain* object in the RDAP response MUST contain an *entity* with the *registrar* role (called registrar entity in this section) and a valid *fn* member MUST be present.

2.4.2. Registrar IANA ID - The *handle* of the *entity* MUST be equal to the IANA Registrar ID.

2.4.3. Registrar IANA ID - The *entity* with the *registrar* role in the RDAP response MUST contain a *publicIDs* member [RFC7483] to identify the IANA Registrar ID from the IANA's Registrar ID registry (https://www.iana.org/assignments/registrar-ids/registrar-ids.xhtml). The type value of the *publicID* object MUST be equal to IANA Registrar ID.

2.4.4. Other members MAY be present in the *entity* (as specified in RFC6350, the vCard Format Specification and its corresponding JSON mapping RFC7095).

2.4.5. Abuse Contact (email, phone) - An RDAP server MUST include an *entity* with the *abuse* role within the registrar *entity* which MUST include *tel* and *email* members, and MAY include other members.

2.5. Reseller - The returned *domain* object in the RDAP response MAY contain an Optional entity with the *reseller* role, if the domain name was registered through a reseller.

2.6. Domain Status

2.6.1. The top-level domain object in the RDAP response MUST contain at least one *status* member [RFC7483].

Commented [A8]: Suggestion 5

Commented [A9]: Suggestion 5

2.6.2. The *status* member value MUST conform to the *Extensible Provisioning Protocol (EPP) and Registration Data Access Protocol (RDAP) Status Mapping* [RFC8056].

2.6.3. A domain name RDAP response MUST contain a *notices* member with a *title* "EPP Status Codes", a *description* containing the string "For more information on domain status codes, please visit https://icann.org/epp" and a *links* member with the https://icann.org/epp URL.

2.7. Contacts

2.7.1. Contact (object) lookups if supported MUST support RDAP lookup requests for *entities* with any role within other objects using the *handle* (as described in 3.1.5 of RFC7482).

2.7.2. If the RDAP service is provided by a registry that does not support contacts (for example thin registries) then the contact entities described in this section are not REQUIRED for the registry.

2.7.3. Processing where subject to the GDPR is defined in the Temporary Specification - Appendix A - Section 2 and processing where not subject to the GDPR is defined in the Temporary Specification - Appendix B - Section 3.

2.7.4. Registrant, Administrative, Technical, Other - The domain object in the RDAP response MUST contain exactly one entity for each of the following roles: ~~entities with the~~ registrant, administrative and technical. For the absence of doubt, one entity may be attributed to one or more roles. The domain object in the RDAP response ~~roles and~~ MAY contain other entities with corresponding roles (such as billing). Unless otherwise specified, all entities MUST include ~~with~~ a handle (ROID of the contact object, <contact:roid>, as defined in RFC5733 for thick registries; a registrar-unique identifier for thin registries) and valid members fn, adr, tel, email (as specified in RFC6350, the vCard Format Specification and its corresponding JSON mapping RFC7095).

~~2.7.3.1.~~ 2.7.4.1. The following RDDS fields used to generate the adr member of the contact entities are REQUIRED to be included in the RDAP response: Street, City, Country.

~~2.7.3.2.~~ 2.7.4.2. The following RDDS fields MUST be included in the adr member of the contact entities if the data exists: Organization, State/Province, Postal Code, Phone Ext, Fax, Fax Ext. If no data

Commented [A10]: Suggestion 28

Commented [A11]: Suggestion 6

exists, the fields SHOULD NOT be included in the adr member.

2.7.5. Redaction - The redaction requirements in this section MUST be applied by registries and registrars where required by section 2.1 of Appendix A of the Temporary Specification; and MAY be applied by registries and registrars where permitted by section 3 of Appendix A of the Temporary Specification; with the following exceptions: (1) MUST NOT be applied by registrars if contact has provided consent to publish contact's data, or if the contact is using a privacy/proxy service; and, (2) SHOULD NOT be applied by registries if contact has provided consent to publish contact's data.

2.7.5.1. Registrant - ~~Where processing is subject to the GDPR, t~~The following elements ~~MUST be~~will be omitted ~~unless consent to publish has been provided and where processing is not subject to the GDPR MAY be omitted~~; the handle, fn and tel members of the (registrant) contact entity and the Street, City, Postal Code, Phone Ext, Fax and Fax Ext fields of the adr member in the entity~~RDAP response~~ object.

2.7.5.2. Administrative, Technical, Other - ~~Where processing is subject to the GDPR, t~~The following elements ~~MUST~~ will be omitted ~~unless consent to publish has been provided and where processing is not subject to the GDPR MAY be omitted –~~: the handle, fn and tel members of the (administrative, technical, other) contact entity and the Organization, Street, City, State/Province, Postal Code, *ISO-3166-1-alpha-2*~~Country~~, Phone Ext, Fax and Fax Ext fields of the adr member in the ~~RDAP response~~entity object.

2.7.5.3. In an RDAP response where elements of the contact entity have been omitted, the contact entity MUST include a remarks element containing a title member with a value “REDACTED FOR PRIVACY” ~~and~~ , a description member with a value “Some of the data in this object has been removed.~~”~~ and a type member with a value "object truncated due to authorization".

2.7.6. Email – The redaction requirements in this section MUST be applied by registries and registrars where required by section 2.1 of Appendix A of the Temporary Specification; and MAY be applied by registries and registrars where permitted by section 3 of Appendix A of the Temporary Specification; with the following exceptions: (1) MUST NOT be applied by registrars if the contact is using a privacy/proxy service; and (2) are OPTIONAL to be applied by registries and registrars if contact has provided consent to publish contact's data.

2.7.6.1. The *EMAIL* property will be omitted. ~~Where processing is subject to the GDPR the following MUST be applied and MAY be applied where not subject to the GDPR.~~

2.7.6.2. Email (Registrar Only) - ~~the value of the email member in the~~

Commented [A12]: Suggestion 25

Commented [A13]: Revised for clarity

Commented [A14]: Suggestion 19

Commented [A15]: Suggestion 12

Commented [A16]: Suggestion 9

Commented [A17]: Revised for clarity

~~RDAP response MUST be an email address~~The registrar MUST provide an ~~or~~ email address or a web form to facilitate email communication with the relevant contact~~link to a webform to facilitate email communication with the Registrant~~ in the *CONTACT-URI* property of the entity object. The email address or link to the webform ~~but~~ MUST NOT identify the contact email address or the contact itself. Note: the *CONTACT-URI* property is pending registration in the IANA vCard Elements Registry.

~~2.7.6.2.~~ 2.7.6.3. Email (Registry Only) - The registry MUST include a remarks element containing a title member with a value "EMAIL REDACTED FOR PRIVACY", a description member with a value "Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant of the queried domain name." and a type member with a value "object truncated due to authorization".

~~2.7.3.3. Email (Registry Only) - the value of the email member in the RDAP response MUST be substantially similar to the following "Please query the RDDS service of the Registrar of Record~~

~~2.7.3.4. identified in this output for information on how to contact the Registrant of the queried domain name."~~

2.7.7. Notwithstanding sections 2.7.5 and 2.7.6 above, registries and registrars MAY provide unredacted registration data as described in Temporary Specification for gTLD Registration Data, Appendix A, section 4 via RDAP.

2.7.8. The RDAP response to a Contact query MUST include an eventAction type *last update of RDAP database* with a value equal to the timestamp when the RDAP database was last updated.

2.8. Name Server(s) - The *domain* object in the RDAP response MUST contain the name servers of the domain in the *nameservers* member.

2.8.1. RDAP servers MUST support *nameserver* lookup queries based on the name server's name as specified in 3.1.4 of RFC7482.

2.8.2. RDAP servers operated by Registries MUST support *nameserver* ~~lookup~~ search queries based on IP address as defined in RFC7482 section 3.2.2. RDAP servers MUST NOT support Partial String Searching as defined in RFC7482 for searching *nameserver* based on IP addresses.

Commented [A18]: Suggestion 15

Formatted: Indent: Left: 1.81", No bullets or numbering

Commented [A19]: Suggestion 26

Commented [A20]: Suggestion 10

Commented [A21]: Suggestion 14

2.8.3. Each *nameserver* object MUST contain the following member: *ldhName*.

2.8.4. The following members are Optional: *ipAddresses* [RFC7483], *unicodeName*, *handle* [RFC7483] (ROID of the host object, *<host:roid>* as defined in RFC5732), and *status*.

2.8.5. In the case of a TLD in which name servers are specified as domain attributes, the *nameserver* object MUST NOT contain the following members: *handle* and *status*.

2.9. DNSSEC - The *domain* object in the RDAP response MUST contain a *secureDNS* member [RFC7483] including at least a *delegationSigned* element. Other elements (e.g. *dsData*) of the *secureDNS* member MUST be included, if the domain name is signed and the elements are stored in the Registry or Registrar database, as the case may be.

2.10. RDDS Inaccuracy - A domain name RDAP response MUST contain a *notices* member with a *title* "RDDS Inaccuracy Complaint Form", a *description* containing the string "URL of the ICANN RDDS Inaccuracy Complaint Form: https://www.icann.org/wicf" and a *links* member with the https://www.icann.org/wicf URL.

2.11. Registrar only requirements - the following requirements apply to registrars only.

2.11.1. A Registrar MUST return an HTTP 404 response when the Registrar is not the Sponsoring Registrar for the domain name.

2.11.2. The *domain* object *handle* in the RDAP response MUST contain the Repository Object Identifier (ROID of the domain object, *<domain:roid>* as defined in RFC5731) for the Domain Name object. For example, a Registrar could obtain the ROID from the Registry via EPP and cache the information locally after creating or gaining a domain name via a transfer.

2.11.3. The *entity handle* in the RDAP response MUST contain the Repository Object Identifier (ROID of the contact object, *<contact:roid>*, as defined in RFC5733) for the Contact object. For example, a Registrar could obtain the ROID from the Registry via EPP and cache the information locally. The RAA 2013 defines that this information MUST be shown if available from the Registry. If this information is not available from the Registry (e.g., a "thin" Registry), the *handle* MUST contain the unique identifier within the Registrar.

2.11.4. The *eventAction* type *last changed* MUST reflect the date and time of the

latest successful update known to the Registrar. Registrars are not required to constantly refresh this date from the Registry.

2.11.5. The *status* element MUST reflect the latest known set of EPP statuses in the Registry. Registrars are not required to constantly refresh the EPP statuses from the Registry.

3. ~~R~~Registry's RDAP server responses to r~~R~~egistrar object queries ~~RDAP queries~~

Note: this section only applies to Registries.

3.1. Registrar object ~~lookup~~ search using an entity query on the *fn* element MUST be supported. RDAP servers MUST NOT support Partial String Searching as defined in RFC7482 for searching *entity* object based on the *fn* element.

3.2. Registrar (name, address, phone number, email) - In response to registrar queries, the returned RDAP response MUST be an *entity* with *registrar* role, with a *handle* and valid elements *fn*, *adr*, *tel*, *email*.

3.2.1. Registrar (Street, City, Country) - The *adr* member in the RDAP response for a Registrar query MUST at least contain the following RDDS fields: Street, City, Country.

3.2.2. Registrar (State/Province, Postal Code, Fax Number) - the following fields are ~~optional~~ Optional in the *adr* member of the RDAP response: State/Province, Postal Code, Fax Number.

3.3. Contacts (Admin, Technical) - The RDAP response SHOULD contain at least two *entities*, with the *administrative* and *technical* roles respectively within the *entity* with the *registrar* role. The *entities* with the *administrative* and *technical* roles MUST contain a *handle* and valid *fn*, *tel*, *email* members, and MAY contain a valid and Optional *adr* element.

3.4. The RDAP response to a Registrar query MUST include an *eventAction* type *last update of RDAP database* with a value equal to the timestamp when the RDAP database was last updated.

4. Registry's RDAP server responses to ~~Nameserver~~ nameserver ~~RDAP~~

Commented [A22]: Suggestion 21

Commented [A23]: Suggestion 21

Commented [A24]: Suggestion 13

Commented [A25]: Suggestion 5

Commented [A26]: Suggestion 5

queries

Note: this section only applies to Registries.

Commented [A27]: Suggestion 21

4.1. Name Server (Name) - In response to Nameserver queries the returned RDAP response MUST include a *nameserver* object and contain a *ldhName* member.

4.2. IP Address(es) - If the name server record includes IP addresses then the *nameserver* object MUST contain a ipAddresses member listing all IPv4 and IPv6 glue records for the Nameserver.

4.3. Registrar (Name, IANA ID) - The Registrar RDDS field is Optional; if present in the response, it MUST be represented as an entity with the registrar role. The handle of the entity with the registrar role MUST be equal to the IANA Registrar ID. If the Registrar does not have an IANA ID then the handle of the entity with the registrar role MUST equal "not applicable". If the Registrar has an IANA ID, then the entity with the registrar role in the RDAP response MUST contain a publicIDs member with a type value equal to the IANA Registrar ID. If the Registrar does not have an IANA ID then the RDAP response MUST NOT contain a publicIDs member.

4.4. The RDAP response to a Name Server query MUST include an *eventAction* type *last update of RDAP database* with a value equal to the timestamp when the RDAP database was last updated.

4.5. If registry supports multiple host objects with the same name, registry MUST support the capability to respond with a set of host objects in response to a name server lookup, no later than one hundred thirty-five (135) days after ICANN gives notice that an RFC defining this capability has been published.

Commented [A28]: Suggestion 16

Appendix A: RDAP IETF Standards

RDAP standards are a set of specifications, which together provide a complete RDAP service. Each specification is briefly described below.

RFC7480 - HTTP Usage in the Registration Data Access Protocol (RDAP)
https://www.rfc-editor.org/rfc/rfc7480.txt
Describes usage of HTTP transport for RDAP, error messages, RDAP extensions, rate limiting and internationalization with URIs.

RFC7481 - Security Services for the Registration Data Access Protocol (RDAP)
https://www.rfc-editor.org/rfc/rfc7481.txt
Covers access control, authentication, authorization, privacy, data confidentiality and RDAP services availability considerations.

RFC7482 - Registration Data Access Protocol (RDAP) Query Format
https://www.rfc-editor.org/rfc/rfc7482.txt
Defines the URL patterns for networks, autonomous systems, reverse DNS, name servers, registrars and entities queries. Also covers help requests, search (wildcards) and internationalization in requests.

RFC7483 - JSON Responses for the Registration Data Access Protocol (RDAP)
https://www.rfc-editor.org/rfc/rfc7483.txt
Defines JSON object classes for domains, name servers, entities, IP networks and autonomous system numbers. Describe answers to help queries, searches, JSON-embedded error codes and truncated answers.

RFC7484 - Finding the Authoritative Registration Data (RDAP) Service
https://www.rfc-editor.org/rfc/rfc7484.txt
Describes a method to find the authoritative server for RDAP data.

Appendix B: Other Technical References

RFC7485 - Inventory and Analysis of WHOIS Registration Objects
https://www.rfc-editor.org/rfc/rfc7485.txt

RFC8056 – Extensible Provisioning Protocol (EPP) and Registration Data Access Protocol (RDAP) Status Mapping
https://tools.ietf.org/html/rfc8056
Describes the mapping of the Extensible Provisioning Protocol (EPP) statuses with the statuses registered for us in the Registration Data Access Protocol (RDAP).

IANA RDAP JSON Values Registry
https://www.iana.org/assignments/rdap-json-values/rdap-json-values.xhtml
This registry defines valid values for RDAP JSON status, role, notices and remarks, event action, and domain variant relation, as defined in RFC7483.

IANA Bootstrap Service Registry for Domain Name Space
https://www.iana.org/assignments/rdap-dns/rdap-dns.xhtml

draft-lozano-rdap-nameservers-sharing-name - Nameserver objects sharing the same name, support for the Registration Data Access Protocol (RDAP)
https://tools.ietf.org/html/draft-lozano-rdap-nameservers-sharing-name
Describes a Registration Data Access Protocol (RDAP) extension that may be used to retrieve the registration information of a particular nameserver object sharing the name with other nameserver objects.

draft-ietf-regext-rdap-object-tag – Registration Data Access Protocol (RDAP) Object Tagging
https://tools.ietf.org/html/draft-ietf-regext-rdap-object-tag
Describes an update to RFC7484 by describing an operational practice that can be used to add structure to RDAP identifiers that makes it possible to identify the authoritative server for additional RDAP queries.

Federated Authentication for the Registration Data Access Protocol (RDAP) using OpenID Connect https://tools.ietf.org/html/draft-hollenbeck-regext-rdap-openid
Describes a federated authentication system for RDAP based on OpenID Connect.

jCard: The JSON Format for vCard
https://tools.ietf.org/html/rfc7095

vCard Format Specification

https://tools.ietf.org/html/rfc6350

EPP Status Code (ICANN)
https://www.icann.org/epp

Draft Final Report from the Expert Working Group on Internationalized Registration Data
https://gnso.icann.org/en/issues/ird/ird-draft-final-10mar15-en.pdf

Study to Evaluate Available Solutions for the Submission and Display of Internationalized Contact Data
https://www.icann.org/en/system/files/files/transform-dnrd-02jun14-en.pdf

Mozilla Included CA Certificate List
https://wiki.mozilla.org/CA:IncludedCAs

Appendix C: Policy References

gTLD Base Registry Agreement
https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm

2013 Registrar Accreditation Agreement
https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

Registry Registration Data Directory Services Consistent Labeling and Display Policy (CL&D),
https://www.icann.org/resources/pages/rdds-labeling-policy-2017-02-01-en

Temporary Specification for gTLD Registration Data –
https://www.icann.org/en/system/files/files/gtld-registration-data-temp-spec-17may18-en.pdf

ICANN Advisories
https://www.icann.org/resources/pages/advisories-2012-02-25-en

Advisory: Clarifications to the Registry Agreement, and the 2013 Registrar Accreditation Agreement (RAA) regarding applicable Registration Data Directory Service (Whois) Specifications (RDDS clarification Advisory)
https://www.icann.org/resources/pages/registry-agreement-raa-rdds-2015-04-27-en

Advisory: Registrar Implementation of the 2013 RAA's Whois Requirements
https://www.icann.org/news/announcement-2013-07-31-en

ICANN Consensus Policies
https://www.icann.org/resources/pages/registrars/consensus-policies-en

Additional Whois Information Policy
https://www.icann.org/resources/pages/policy-awip-2014-07-02-en

Final Report on the Thick Whois Policy Development Process
https://gnso.icann.org/en/issues/whois/thick-final-21oct13-en.pdf

ICANN Whois Marketing Restriction Policy
https://www.icann.org/resources/pages/registrars/consensus-policies/wmrp-en

Appendix D: RDDS Fields (data element mappings)

Commented [A29]: Suggestion 11

Domain Name Responses:

RDDS Field	RDAP Response Element
Domain Name	ldhName
Registry Domain ID	handle
Updated Date	events.eventAction “last changed”
Creation Date	events.eventAction “registration”
Registry Expire Date	events.eventAction “expiration”
Domain Status	status object
Name Server	nameservers.ldhname
DNSSEC	secureDNS object
Internationalized Domain Name	unicodeName
Last update of ~~RDS~~ WHOIS ~~D~~database	Events.eventAction “last update of RDAP database”

Registrar	**Entities.role registrar**
~~Sponsoring~~ Registrar	jCard fn~~Entities.roles.registrar~~
~~Sponsoring~~ Registrar IANA ID	publicIDs.identifier
Registrar Abuse Contact Email	Entities.role abuse email
Registrar Abuse Contact Phone	Entities.role abuse phone
Registrar Registration Expiration Date	events.eventAction “registrar expiration”
Registrar ~~RDS~~ WHOIS Server	Links.object with rel:related
Registrar URL	n/a
Reseller	Entities.roles reseller
Registrant	**Entities.role registrant**
Registry Registrant ID	Entity.handle
Registrant Name	jCard “fn”
Registrant Organization	Org
Registrant Street	Grouped into adr member
Registrant City	

Registrant State/Province	
Registrant Postal Code	
Registrant Country	
Registrant Phone ~~Number~~	Tel type parameter voice
Registrant Phone ~~Number~~ Ext	Ext
Registrant Fax	Tel type parameter Fax
Registrant Fax Ext	Ext
Registrant ~~e~~Email	Email
Admin Contact	**Entities.role Administrative**
Registry Admin ID	Entity.handle
Admin Name	jCard “fn”
Admin Organization	Org
Admin Street	Grouped into adr member
Admin City	
Admin State/Province	
Admin Postal Code	
Admin Country	

Admin Phone ~~Number~~	Tel type parameter voice
Admin Phone ~~Number~~ Ext	Ext
Admin Fax	Tel type parameter Fax
Admin Fax Ext	Ext
Admin ~~e~~Email	Email
Technical Contact	**Entities.role Technical**
Registry Tech ID	Entity.handle
Tech Name	jCard “fn”
Tech Organization	Org
Tech Street	Grouped into adr member
Tech City	
Tech State/Province	
Tech Postal Code	
Tech Country	
Tech Phone ~~Number~~	Tel type parameter voice
Tech Phone ~~Number~~ Ext	Ext
Tech Fax	Tel type parameter Fax

Tech Fax Ext	Ext
Tech ~~e~~Email	Email

Registrar Responses:

RDDS Field	**RDAP Response Element**
Registrar	jCard fn
~~Registrar~~ Street	Grouped into the adr member
~~Registrar~~ City	
~~Registrar~~ State/Province	
~~Registrar~~ Postal Code	
~~Registrar~~ Country	
~~Registrar~~ Phone Number	Tel with a type parameter voice
~~Registrar~~ Fax Number	Tel with a type parameter fax
~~Registrar~~ Email	email
Registrar ~~a~~Admin/~~t~~Technical ~~e~~Contact	Entity.role administrative or technical
A~~a~~dmin~~istrative~~/~~t~~Technical ~~e~~Contact	jCard fn
~~Contact~~ Phone Number	Tel with a type parameter voice
Phone Ext	Ext

~~Contact~~ Fax Number	Tel with a type parameter fax
Fax Ext	Ext
~~Contact~~ Email	email
Registrar WHOIS Server / ~~Referral~~ Registrar URL	n/a
Last update of WHOIS database	events.eventAction “last update of RDAP database”

Name Server Responses:

RDDS Field	**RDAP Response Element**
Server Name	nameserver.ldhName
IP Address	nameserver.ipAddresses
Registrar	Entities.roles registrar
Registrar WHOIS Server / ~~Referral~~ Registrar URL	n/a
Last update of ~~RDAP~~ WHOIS database	events.eventAction “last update of RDAP database”