**Registrar Stakeholder Response to the RDAP Response Profile,
the RDAP Technical Implementation Guide, and
ICANN org's input to the Contracted Parties' gTLD RDAP Profile Proposal**

The Registrar Stakeholder Group (RrSG) appreciates the opportunity to provide feedback on the RDAP Response Profile Proposal, RDAP Technical Implementation Guide, and ICANN org's input to the Contracted Parties' gTLD RDAP Profile Proposal. Our feedback is inline below.

RDAP Response Profile Proposal

First and foremost, the RrSG wants to underscore the importance of ICANN vetting all community feedback received regarding this protocol to ensure changes are technically and operationally feasible prior to ICANN's acceptance and incorporation into any final product. All too often well intended ideas are put forward without significant examination of technical and operational feasibility. It is for this reason that the RrSG is strongly stating below its complete opposition to ICANN Org's Input #27 to 'require implementation of searchability in RDAP once an RFC provides such functionality'. This recommendation lacks not only technical feasibility, but also a legal one.

Given the importance this new protocol will play, it is of utmost importance that community recommendations go through a thorough vetting process prior to inclusion in the final RDAP Profile.

It is our understanding that this Profile is specific to the Temporary Specification adopted on 17 May 2018 and additional RDAP Profiles will need to be created in response to EPDP outcomes and/or GNSO policy development. To that end, the RrSG is pleased with the recommendations set forth in the RDAP Profile.

RDAP Technical Implementation Guide

The Registrar Stakeholder Group (RrSG) is satisfied with the guidance provided in this document.

ICANN org's input to the Contracted Parties' gTLD RDAP Profile Proposal

The Registrar Stakeholder Group (RrSG) appreciates the opportunity to provide feedback on ICANN org's input to the Contracted Parties' gTLD RDAP Profile Proposal.

The RrSG feedback is inline below:

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.

RESPONSE: We disagree with ICANN org's use of MUST. The RrSG would encourage the use of SHOULD or MAY, not MUST. Additionally, saying it must be a well-known browser or well-known CA is problematic and nonspecific. Clarity is needed here, either via better definitions (e.g. "well-known"), provide specifics regarding what you are looking for or a reference to a CA Certificate Program's list of included root certificates (ie https://wiki.mozilla.org/CA/Included_Certificates).

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 format for domain and name server 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.

RESPONSE: No issue.

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.

RESPONSE: No issue.

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.

RESPONSE: No issue.

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.

RESPONSE: Disagree. If the field is optional it should not have to be displayed, regardless if it is blank of not.

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.

RESPONSE: RDAP Profile shouldn't be defining how many contacts should be allowed/required. The contacts may vary by business model and it should be left to each registrar/registrant to determine.

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.

RESPONSE: No issue.

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.

RESPONSE: Policies should not be stated/named out here. While we do not disagree, listing it here is unnecessary.

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.

RESPONSE: Agree. This is a business decision and MAY be done but should not be mandatory.

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.

RESPONSE: RDAP is a protocol, not a database. It should be the "last update of the registrar/registry database."

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.

RESPONSE: Policies should not be stated/named out here. While we do not disagree, listing it here is unnecessary.

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.

RESPONSE: There should be a list of reasons: Redacted for Privacy, Truncated due to load, etc.

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.

RESPONSE: Agree.

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.

RESPONSE: Agree.

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.

RESPONSE: This doesn't fit with the current profile. It could be integrated into future profiles once other technical hurdles have been resolved. This appears to simply support consumers of data and is beyond the scope of our responsibility.

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.

RESPONSE: It is unclear how this is supposed to work or how this is possible. Further clarity is needed.

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.

RESPONSE: No problem if this is a MAY.

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.

RESPONSE: No issue.

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.

RESPONSE: We agree it should be in there but not until a vCard property supports it.

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.

RESPONSE: No issues.

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.

RESPONSE: No issue.

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.

RESPONSE: Disagree. What is proposed is a top down process (not a bottom up multi-stakeholder process) and injects new policy via an RFC solution.

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.

RESPONSE: Agree.

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.

RESPONSE: This should be optional. You MAY omit.

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.

RESPONSE: Policies should not be stated/named out here. While we do not disagree, listing it here is unnecessary.

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.

RESPONSE: This belongs under Unified Access Model ("UAM") not in the RDAP Profile. Again, this is a policy issue and doesn't belong in a Profile.

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.

RESPONSE: ***<u>The RrSG does not support this proposal.</u>*** ***This is not technically (or legally) feasible due to the level of burden and risk placed on the registrar. It does not scale and does not provide discernable value for current valid use cases. Also, it is not clear how ICANN, as a data controller, would be able to demonstrate compliance with Art 25 and Art 35 of the GDPR.***

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.

RESPONSE: RrSG does not support and should not be required to create a unique identifier.