MarkMonitor
Protecting brands in the digital world

Clarivate Analytics

MarkMonitor Comment on Proposed gTLD Registration Data Access Protocol (RDAP) Profile

Dear ICANN,

We appreciate the opportunity to comment on the proposed RDAP profile. With specific comments following below, we also comment generally that in the interest of consistent and reliable contracted party implementation, more time to implement is desirable, as opposed to less, and we're aware that a number of contracted parties have expressed concern about the ability to implement this in the proscribed 135-day window. We also note generally that the vCard/jCard standard for general purpose contact information is a poor fit for domain name registration data as it requires designation of data, such as a "work address" or a "home phone". As a stand-alone item, a jCard document is easy to deal with, as many libraries exist to transform the format, but its inclusion within a larger JSON body makes serialization/deserialization difficult as it's less practical to extract the jCard body to use with an existing library, versus serializing it manually. As a final general matter, we ask whether, and for how long, contracted parties should publish both WHOIS and RDAP concurrently; will WHOIS and RDAP both output the same RDS information indefinitely?

Please see below our feedback on specific sections of the RDAP profile currently posted for community input.

Item 1. RDAP servers should use a TLS server certificate from a well-known Certificate Authority (CA). Securing the RDAP servers is important, and may be required by the GDPR, among other local privacy laws.

Item 2. In the interest of promoting the use of IDNs, RDAP servers should support queries in U-label format.

Item 3. While we do not feel strongly about this, referring to our comment on Item 2, we do not think that RDAP servers should reject such queries. We anticipate RDAP servers may not persist the syntax of the query in the response, and we accept that reality.
U-label.a-label = OK: 警備.net
LDH.u-label = NOT OK: xn--s34lkser.警備

Item 4. With reference to our general note above, this indicates rushed RDAP implementation. Specifically to this point, if we can securely enable a web based javascript RDAP client, then we should. We would expect that supporting this header would be a web server configuration, as opposed to requiring implementation that's complex and/or novel.

Item 5. RDAP servers should be required to return optional fields that contain data. This protects registrants who have opted in to having data published.

Item 6. The RDAP profile must follow policy, and if policy does not prohibit multiple contacts, registrants should be allowed to provide them.

Item 7. To help facilitate the adoption of accredited access, we support including the version of the RDAP profile supported in the response.

Item 8. Yes, RDAP extensions and additional fields requirements must be consistent with established policy.

Item 9. Registrants must have the choice of opting in for the publication of full contact data (including email), even when subject to GDPR, and 2.7.6 must be revised to make this clear.

Item 10. We support requiring this event, consistent with established policy.

Item 11. We support mapping that is consistent with the Consistent Labelling & Data ("CL&D") Policy.

Item 12. We support including the remarks element as it enables maintaining the data integrity of the fields (i.e. “no data in a field is better than bad data”). To be clear, contrary to the Temporary Specification, no data should be returned when the field has been redacted. We also support the addition of a new value for the type to convey redaction accurately as distinct from truncation. The remark element’s most powerful feature could be to contain the link to the registrant contact form on the registrar’s website when no email address is in the field. This could improve the integrity of the registrant email address field by requiring it to be an email address, or to be blank, and not to be a link.

Item 13. This is minimally used, but we support ICANN’s suggestion.

Item 14. Doing an IP address search versus hostname lookup makes sense, since there can be many name servers using the same IP address. Ensure both IPv4 and IPv6 addresses can be specified for a nameserver lookup.

Item 15. See our response to Item 12 above for a better solution that does not require changing vCard elements.

Item 16. We don’t want to query host objects, or respond to host object queries, in non-sponsoring TLDs. For example, we shouldn’t query or respond to ns1.example.com inside the .org namespace.

Item 17. Without commenting on whether RFC 7483 is good variant policy, we should include a “may” here to establish a placeholder for future policy.

Item 18. Roles must be registered with IANA.

Item 19. We strongly support the use of ISO-3166 country codes using the addition of the “cc” property to the vCard/jCard address object. This will help support localized data processing requirements based on local privacy requirements.

Item 20. In the interest of promoting the use of IDNs, we agree that RDAP should support LDH names in queries and responses.

Item 21. This is ok.

Item 22. We agree in principle, and note that time-boxing could be problematic for RFC implementation requirements that prove more onerous than others.

Item 23. We agree that registries must provide a referral link to the sponsoring registrar so queries can always follow from the registry to the registrar. Registrars should not provide a referral to themselves to prevent infinite referral loops.

Item 24. RDAP clients could be simplified if a Unicode field and an ACE field were both always represented in the JSON output. For example, “domainName” would always be the U-label representation (or A-label if ASCII-only) while “domainNamePunycode” would always be the ASCII character encoding, which would duplicate the A-label if ASCII-only, or represent the U-label in punycode format for a Unicode domain. User-friendly RDAP clients would then always show the “domainName” field as the prominent representation, and only if the “domainNamePunycode” value was different, display its value to the user (perhaps in a smaller font or UI distinguishing way). This promotes general acceptance of IDNs.

Item 25. We agree that privacy/proxy contact information should not be redacted (i.e. the privacy/proxy information in the data fields should be returned in response to an RDAP query and not left blank). We would also propose (or support) an RDAP element indicating whether P/P is in use or not, in accordance with II.4 of the Final Report on the Privacy & Proxy Services Accreditation Issues Policy Development Process.

Item 26. We agree that the RDAP Profile itself must not prohibit access to registration data. RDAP must support “reasonable access” under the Temporary Specification, as well as “UAM” access under future policy.

Item 27. Search queries must have different SLAs than exact match queries.

Item 28. Is this a single identifier per registrar? How would the registrar set this at the registry? Which party (Ry/Rr) is responsible for displaying this, perhaps both? Pilot group has not yet discussed this.

We are available to discuss further at your convenience.

Sincerely,

Brian King & Justin Mack
MarkMonitor Policy Team, with special thanks to Alex Deacon of Cole Valley Consulting