Comments from Mohit Batra on - "Proposed gTLD-Registration Data Access Protocol (RDAP) Profile"

Please note that these comments are purely in my personal capacity, and don't represent the views of my employer.

Comments from Mohit Batra (MB):

1. Since RDAP services are based on RESTful web services architecture, due care must be taken by ICANN and contracted parties (gTLD Registries and Registrars) regarding secure usage and deployment of RDAP. Industry best practices and guidelines (e. g. REST Security Cheat Sheet from OWASP) may be utilized for the same.

https://www.owasp.org/index.php/REST_Security_Cheat_Sheet

Web Application Firewalls (WAFs) also may be deployed at RDAP servers' end (Registries/Registrars end) to prevent abuse and hacking attempts.

2. An analysis of the impact of proposed gTLD-Registration Data Access Protocol (RDAP) Profile on the rollout of ICANN's Privacy/Proxy Services Accreditation programme needs to be done, as it can be observed that GNSO PDP on Privacy/Proxy Services is in final stages of completion.

https://gnso.icann.org/en/group-activities/active/ppsai

3. A FAQ document on Proposed gTLD-Registration Data Access Protocol (RDAP) Profile may be prepared with questions, some of which are stated below:

a) What are knowledge pre-requisites for deploying RDAP across gTLDs

Ans - HTTP, JSON, TLS, RESTful Web Services, EPP, RDAP RFCs, Web Applications and its Security etc

b) Which gTLD RDAP profile requirements apply to registries only, registrars only, both

c) Do Privacy/Proxy Services providers and Resellers need to deploy RDAP services?

d) Are there any case studies on RDAP deployment for numbering resources by RIRs?

etc.

4. RDDS Consistent Labelling and Display Policy "main" web page (https://www.icann.org/rdds-labeling-display) displays obsolete/rescinded policy, while "another" ICANN webpage (https://www.icann.org/resources/pages/rdds-labeling-policy-2017-02-01-en) has "latest" policy.

Notably, a quick Google search on "Registry Registration Data Directory Services Consistent Labeling and Display Policy" has 1st result for rescinded policy page, while "latest" policy is not visible on Google search results page.

For consistency sake, results of "latest" policy should be moved to URL https://www.icann.org/rdds-labeling-display

5. A case study or status-quo regarding deployment/usage of RDAP RFC specifications for Regional Internet Registries (RIR's) and National Internet Registries (NIR's) needs to be done. This analysis for Numbering resources (by RIRs / NIRs) will surely benefit Domain Name Industry (i.e. contracted parties) in their successful implementation of gTLD RDAP profile.

It is also to be noted that RIR's such as RIPE NCC and ARIN were the first ones to experiment with RESTful Web Services for WHOIS queries, which eventually led to standardization of RDAP RFC's (RFC 7480-85) by IETF WEIRDS Working Group.

Thanks & Regards,
Mohit Batra
Certified Information Systems Security Professional (CISSP)
Member - ICANN RSSAC caucus

ICANN and IETF fellow
Technology Analyst
National Internet Exchange of India
www.nixi.in
www.mohitbatra.in
Twitter: https://www.twitter.com/mohitbatra80
LinkedIn: https://www.linkedin.com/in/mohitbatra80/