RDAP status

Edward Lewis | APTLD 2016 | February 2016
The Registration Data Access Protocol (RDAP) is a protocol designed to replace the existing WHOIS protocol and provides the following benefits:

- Internationalization support for registration data (e.g., contact names in Chinese)
- Standardized query, response, and error messages
- Extensibility (e.g., easy to add output elements)
- Secure access to data (i.e., over HTTPS)
- Bootstrapping mechanism to easily find the authoritative server for a given query
- Standardized redirection/reference mechanism (e.g., from a thin registry to a registrar)
- Builds on top of the well-known web protocol HTTP (e.g., eases implementation of the RDAP services by leveraging existing knowledge to run web services)
History on Replacing the WHOIS Protocol

- SSAC’s SAC 051 (19 Sep 2011): *The ICANN community should evaluate and adopt a replacement domain name registration data access protocol*
- Board resolution adopting SAC 051 (28 Oct 2011)
- Roadmap to implement SAC 051 (4 Jun 2012)
- RDAP community development within IETF WG began in 2012
- Contractual provisions in: .biz, .com, .info, .name, .org, 2012 Registry Agreement (new gTLDs), 2013 Registrar Accreditation Agreement
- RDAP Request for Comments (RFCs) published (Mar 2015)
- First draft gTLD RDAP profile mapping current contractual and policy obligations posted for public input (Sep 2015)
- Second draft of gTLD RDAP profile posted for comment (3 Dec 2015)
ICANN gTLD RDAP Profile

RDAP RFCs:
- SHOULDs, MAYs, MUSTs
- Do not specify required data elements

ICANN gTLD policies

RDDS provisions in the RA, RAA 2013, Whois advisory
RDAP implementation in ccTLDs

- Registro.br (.br) is providing an RDAP service, more information at: http://registro.br/rdap/
  - A client: https://github.com/registrobr/rdap-client

- DNS Belgium (.be)
  - https://github.com/DNSBelgium/rdap

- RDAP is in use by the Regional Internet Registries
  - https://www.apnic.net/apnic-info/whois_search/about/rdap
  - https://www.arin.net/resources/whoisrws/
RDAP allows for Registry Policy to define what should be in the output.

The default protocol (without extensions) supports most of the data elements found in gTLDs (Whois).
Opensource RDAP implementations

- CNNIC RDAP server
  - https://github.com/cnnic/rdap

- RIPE-NCC RDAP server
  - https://github.com/RIPE-NCC/whois/tree/rdap
RDAP abuse prevention mechanisms

- RDAP supports differentiated access, therefore the information exposed to authenticated users could be different to non-authenticated users, thus limiting the information that could be harvested by data miners.

- RDAP uses http as a transport mechanism, therefore all the libraries / modules used to mitigate abuse / attacks in HTTP can be easily used in RDAP.
Thank You and Questions
Reach us at: globalSupport@icann.org
Website: icann.org

Engage with ICANN
twitter.com/icann
gplus.to/icann
facebook.com/icannorg
weibo.com/ICANNorg
linkedin.com/company/icann
flickr.com/photos/icann
youtube.com/user/icannnews
slideshare.net/icannpresentation