RDAP Implementation in the gTLD Space

Tech Day

Francisco Arias

ICANN 63
22 October 2018
Agenda

- Introduction
- RDAP Implementation Status in gTLDs
- Next Steps
Introduction
Issues with (port-43) WHOIS

- No standardized format
- Lack of Support for Internationalization
- Unable to authenticate and thus provide different outputs depending on the user
- Lookup only; no search support
- Lack of standardized redirection/reference
- No standardized way of knowing what server to query
- Insecure
  - No way to authenticate the server
  - No way to encrypt data between server and client
Chronology of RDAP Implementation [1/2]

- **19 September 2011**: SSAC’s SAC 051: “The ICANN community should evaluate and adopt a replacement domain name registration data access protocol“

- **28 October 2011**: Board resolution adopts SAC 051

- **4 June 2012**: Roadmap to implement SAC 051 is published

- **2012**: RDAP community development within IETF WG begins

- **March 2015**: RDAP IETF RFCs are published

- **June 2015**: work on the RDAP gTLD Profile which maps RDAP features to existing policy and contractual requirements begins

- **26 July 2016**: Version 1.0 of RDAP gTLD Profile is published
Chronology of RDAP Implementation [2/2]

- **9 August 2016**: The RySG submitted a “Request for Reconsideration” regarding the inclusion of RDAP in the Consistent Labeling & Display policy, among other things.

- **1 February 2017**: A revised Consistent Labeling & Display Policy, removing the RDAP requirement was published.

- **1 August 2017**: ICANN org received a proposal from the RySG with support from the RrSG to implement RDAP.

- **1 September 2017**: ICANN org responded to the RySG accepting the proposal.

- **25 May 2017**: The Temporary Specification for gTLD Registration Data calls for gTLD registries and registrars to implement RDAP following a common profile, SLA, and registry reporting.
The Registration Data Access Protocol (RDAP) is a protocol designed in the IETF (RFCs 7480 - 7484) to replace the existing WHOIS protocol and provides the following benefits:

- Standardized query, response and error messages
- Secure access to data (i.e., over HTTPS)
- Extensibility (e.g., easy to add output elements)
- Enables differentiated access (e.g., limited access for anonymous users, full access for authenticated users)
RDAP Features [2/2]

- Bootstrapping mechanism to easily find the authoritative server for a given query
- Standardized redirection/reference mechanism (e.g., from a registry to a registrar)
- Builds on top of the well-known web protocol, HTTP
- Internationalization support for registration data
- Enables searches for objects (e.g., domain names)
RDAP Implementation Status in gTLDs
Implementation Status

- The Temporary Specification for gTLD Registration Data calls for gTLD registries and registrars to implement RDAP following a common profile, SLA, and registry reporting requirements.

- A proposal for a gTLD RDAP Profile ended its public comment period on 13 October 2018.

- ICANN org and the contracted parties continue to negotiate an RDAP SLA and registry reporting requirements.
### Draft gTLD RDAP profile
- **13 Oct 2018**: Draft gTLD RDAP profile ended
- **Public Comment**

### Publish draft gTLD RDAP SLA, and registry reporting requirements for Public Comment
- **Oct 2018**: Publish draft gTLD RDAP SLA, and registry reporting requirements for Public Comment

### Publish Final gTLD RDAP profile
- **Nov-Dec 2018**: Publish Final gTLD RDAP profile

### Publish Final gTLD RDAP SLA, and registry reporting requirements
- **Dec 2018**: Publish Final gTLD RDAP SLA, and registry reporting requirements

### RDAP service becomes generally available
- **1H 2019**: RDAP service becomes generally available

### Expected Implementation Timeline
- **135-day Implementation Period**
- **Public Comment Period**

---

*ICANN*
Next Steps
Differentiated Access

- The Temporary Specification for gTLD Registration Data sets the basis for differentiated access by defining a minimum output and requiring contracted parties to provide access to further data on the basis of a legitimate interest.

- Further policy work/requirements have to be developed in order to have a Unified Access Model that would provide for this access in a consistent way in the gTLD space.

- On the technical side, authentication/authorization technologies have to be chosen in order to have a unified implementation.
RDAP Client

- API for technical and frequent users:
  - RDAP by itself provides this

- Command line for technical, non-frequent users:
  - There are a couple of freely available clients
  - Ultimately, web crawlers (e.g., curl, wget) with some JSON formatter could be enough

- Web interface for the non-technical users providing "human-friendly" HTML output:
  - ICANN likely interested to offer one; maybe others?
  - Un-authenticated queries work if "Access-Control-Allow-Origin" header included (RFC 7480, §5.6 recommends it)
  - Authenticated queries may or may not work depending on the authentication technology
Resources

- RDAP page: [https://icann.org/rdap](https://icann.org/rdap)
- Pilot page: [https://community.icann.org/display/RP/RDAP+Pilot](https://community.icann.org/display/RP/RDAP+Pilot)
  - Six registries covering 50+ gTLDs
- Mailing list: [https://mm.icann.org/mailman/listinfo/gtld-tech](https://mm.icann.org/mailman/listinfo/gtld-tech)
Engage with ICANN

Thank You and Questions

Visit us at icann.org
Email: globalSupport@icann.org

@icann
facebook.com/icannorg
youtube.com/icannnews
flickr.com/icann

linkedin/company/icann
slideshare/icannpresentations
soundcloud/icann
instagram.com/icannorg