RDAP in the gTLD Space

Putting all the Pieces Together

Francisco Arias

ROW - Vancouver
17 May 2018
Agenda

- Background
- Server side
- Other components
- Client side
- When?
- How to participate
Background
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
Background

- **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
Background

- **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.

- **Upcoming**: GDPR compliance may require differentiated access to registration data.
Server Side
Server Side RDAP

- RDAP specification was standardized since 2015 (RFCs 7480-84, 8056)
- Open source RDAP server implementations available
- Consistent RDAP responses via gTLD RDAP profile(s)

Draft GDPR compliance model for gTLDs requires RDAP for gTLD registries and registrars
  - Registries/registrars implementing RDAP “their way”
  - Consistent approach by the end of the year
  - Do we need to extend searchability in RDAP?
gTLD RDAP Profile(s)

- Defines common elements to appear in gTLD registry and registrar RDAP responses
- Contains technical elements (e.g. HTTPS only, TLS requirements, IPv4/6 transport, truncated responses behavior, reference mechanism from registry to registrar, format options for elements)
- Maps contractual and policy requirements to RDAP elements (e.g., which fields to show to whom, which elements to be present, supported types of queries)
Other Components
Other Components

- Authentication/authorization technology; currently considering:
  a) Federated Authentication for RDAP using OpenID Connect
  b) Digital Certificates
  - How do we decide which to implement?

- Accreditation model to decide who gets access to what
  - Some community members working on a proposal
  - ICANN org and Community to agree on a model
Client Side
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
Web Client and the Authentication Technology

- Assumption: the web server providing the web client should not have access to any of the following: query, response, or credentials

- Web client behavior with client certificates:
  - Possible if RDAP servers include the “Access-Control-Allow-Credentials” header
  - Is this acceptable?

- Web client behavior with OpenId Connect:
  - Server providing web client would have access to authentication code (a temporary credential)
  - Is this acceptable?
When?
gTLD RDAP Profile(s) Draft Timeline

- 5 Sep 2017
  - RDAP Pilot began
  - Work on gTLD RDAP profile(s) began

- 17 May 2018
  - GDPR Temp Spec

- 31 Jul 2018
  - gTLD RDAP profile(s) finalized
  - Auth tech selected?

- Mid-Dec 2018
  - RDAP service goes in production including client-side

- TBD
  - Accreditation Model

Draft
How to Participate

- RDAP page: https://icann.org/rdap
- Pilot page: https://community.icann.org/display/RP/RDAP+Pilot
  - Six registries covering 50+ gTLDs
- Mailing list: 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