Technical Study Group on Access to Non-Public Registration Data
DRAFT Charter

20 December 2018
Revised 16 January 2019
Revised 13 February 2019

Purpose

This group will explore technical solutions for authenticating, authorizing, and providing access to non-public registration data for third parties with legitimate interests. The work is focused on examining technical implementation solutions built on the Registration Data Access Protocol (RDAP). In parallel with community efforts to develop an RDAP profile prior to deployment of the protocol, this Technical Study Group will focus its efforts on developing technical solutions for providing access to non-public data. At the conclusion of its work, the group will share its findings/proposed specification with the ICANN organization and the ICANN community, in parallel with efforts to implement RDAP.

In a blog published 24 September, ICANN President and CEO Göran Marby wrote that ICANN is exploring possible technical solutions to be built on RDAP. This approach, upon which the Technical Study Group will begin their discussion was further described during a data protection/privacy update webinar held 8 October. The implementation approach described during that webinar would place ICANN in the position of determining whether a third party's query for non-public registration data ought to be approved to proceed. If approved, ICANN would ask the appropriate registry or registrar to provide the requested data to ICANN, which in turn would provide it to the third party. If ICANN does not approve the request, the query would be denied.

The group will not make decisions or recommendations on policy questions, e.g., who gets access, to which data fields and under what conditions should access be given, and what is a legitimate interest for requesting such data. The group will likely consider the technical impact of policy choices, for example, policy recommendations that arise from the Expedited Policy Development Process or other policy initiatives. Where there are multiple alternatives in either the recommended policy(ies) or the technical implementation(s), the group will strive to support options from which choices can be finalized later.

Background

With its adoption of the Temporary Specification for gTLD Registration Data, the ICANN Board of Directors noted in the Annex as an important issue for further community action the development of "an accreditation and access model that complies with GDPR, while recognizing the need to obtain additional guidance from Article 29 Working Party/European Data Protection Board." The EPDP, as part of its charter, plans to consider a standard access mechanism after answering a series of gating questions. To assist the community in its policy development work, ICANN org produced the Draft Framework for a Possible Unified Access Model as a starting point for conversations with European data protection authorities, including the European Data Protection Board.

In addition, the Temporary Specification also directed the creation of a gTLD Registration Data Access Protocol (RDAP) profile as a prerequisite to launching the RDAP service across the gTLD space. ICANN org recently closed a public comment period on a proposal for a profile from a discussion group of gTLD registries and registrars with which it worked to develop the profile. This work will be key to the development of a technical solution for providing third parties with a legitimate purpose with access to non-public registration data.

Assumptions

The group will base its work on the following assumptions:

1. RDAP is the model used to access registration data; port 43 will be deprecated.
2. A standard model will apply equally to all parties requesting access to non-public registration data
3. ICANN is the sole party that authorizes access to non-public registration data in the gTLD space.
4. System will accommodate changes to data sets or data access.
5. All credentials must be protected in a reasonable way.
6. For the purposes of access to non-public data, scope is limited to RDAP, extension mechanisms to RDAP as defined by RFC 7480, 7481, 7482, and 7483, and other mechanisms an RDAP client implementer would find "natural" to implement.
7. It is expected that RDAP services will answer queries from unauthenticated sources, and when doing so will follow policies whereby data is redacted such as those listed in the Temporary Specification for gTLD Registration Data.
8. The solution will take into consideration the existing practices and currently deployed uses of RDAP.
9. The RDAP profile WG will complete its RDAP profile work, and such output is ratified through the appropriate processes.
10. Data holders assume that ICANN will ensure validity of credentials.
11. Requestors must process data in accordance with the Information Security requirements (i.e., Section 8 in TSG's Requirements document).

Commented [1]: Added per discussion at Jan. F2F

Commented [2]: Added per discussion at Feb. F2F

12. In consideration of the Right to be forgotten (Article 17, GDPR), the system is not envisaged to keep personal data, Right to be forgotten should be referred to contracted parties.
13. Policy choice may change the technical implementation of the proposed draft technical model.
14. If adopted, the draft technical model will require more work to become an implementable specification.

Commented [3]: Need to relook at the language. Needs both legal and policy group review from within ICANN Org

Commented [4]: Added per discussion at Feb F2F

Key Questions

The group will consider the following key questions:

Assessment of Available Tools & Protocols

1. Track ongoing development of the RDAP profile.

Authentication/Authorization

1. What technical method would ICANN use to approve a third-party's request for non-public registration data?
2. How could an online, interactive authorization request work?
3. How could an asynchronous-authorization request work?
4. How could authentication of the requestor work considering a decentralized approach for authenticating bodies?

Data Transport/Storage & Audit

1. For queries that are required to be logged, how would a specification allow choices on who would log such queries and how such logging could be done?
2. How could a query that is required not to be logged be identified as such?
3. How could access be provided to authorized parties when it is decided who/how/when logs may be accessed?

Access Control Protocol

1. How could a centralized authorization interface operated by ICANN work? Should this include delegation?
2. How could access to non-public registration data be granted only to clients that are authorized by ICANN?
3. How could ICANN, in its role as the authorizing party, receive a third-party request for access to non-public registration data?
4. Categorization/prioritization of RDS data fields: Should all the fields be collected in one place? If so, should we design a protocol that allows for the categorization of these fields and the prioritization of the request response?

Performance Requirements

1. What are the performance and scalability requirements?
2. How should the service perform in request/response mode?
3. How should the service perform in queueing?
4. How should the service manage extensibility?
5. What are the security requirements?
6. What are the reliability/resiliency requirements?

Other Key Issues for Discussion

- *Transparency, assignment of responsibility*: The proposed specification should be as transparent as possible, with logging of all information entered into the protocol, as well as all instances of access to information. The logging itself must also be in a form that is easily accessed. The specification should allow for exceptions to the logging described above.
- *Error conditions*: Errors are unavoidable, but may be mitigated against with proper planning. The Technical Study Group will consider four broad sources of errors:
    - System errors, security: Failures of operation or procedures for the system. Everything from hardware and software bugs to security breaches. Include in the design what to do when these things happen.
    - Information collection errors (registrants and registrars): The people, processes and systems involved in collecting information will face challenges. The system must be carefully designed to determine what information it accepts and what it does when there are mistakes. The group will attempt to list how errors may be made during this process.
    - Information access errors: Similarly, the people, processes and systems involved in accessing information will likely face challenges. The system should be designed to consider how to process malformed requests. If the requesting parties exceed their authority or improperly disseminate the information they have retrieved, make sure it's possible to delineate system errors between ICANN's systems and third party systems.
    - Policy based errors: Defined policy disallows the requested data to be disclosed
- *Accounting, costs, billing*: Policy discussions have touched on payments for look-ups and transactions. The specification should consider how to accommodate billing models.
- *Maintenance and evolution*: This won't be a static system. The group should consider which parties will be responsible for maintenance and whether that is maintenance of the entire system or specific portions.
- *Governance*: There will be a continuing need for two levels of oversight: technical oversight to ensure that the technology is responsive to policy recommendations.
- *Multi-use requests*: How to handle requests from authorized parties that may be either single-domain or multi-domain, or on a different purpose basis, on demand?

Team Composition

The group will be composed of invited members with technical backgrounds, including expertise in RDAP and authentication/authorization technologies.

Role	Name
Coordinator	Ram Mohan
Team Members	Benedict Addis Gavin Brown Jorge Cano Steve Crocker Scott Hollenbeck Jody Kolker Murray Kucherawy Andy Newton Tomofumi Okubo
ICANN Org Support Team	John Crain (OCTO) - Technical advisor, including security Francisco Arias (GDD) - Technical advisor, including contracted parties Eleeza Agopian (MSSI) - Content development/communications Erika Randall (Legal) - Legal advisor Diana Middleton (MSSI) - Project manager

Deliverables/Timeline

1. Confirm the categories are right: Group to discuss categories of key questions and determine whether they are appropriately grouped.
2. Discuss questions in each category and define any dependencies/stubs.
3. Review tools and protocols that may be available in each category.
4. Define use cases.
5. Determine the design requirements.
6. Create draft architecture/stack for discussion.
7. Create workflow to identify dependencies/bottlenecks.
8. Conduct review of 4, 5, 6 to see if we are on track.
9. Look for rough consensus.Write draft spec.
10. Determine appropriate group of technical experts with whom to vet the draft spec.
11. Vet draft spec.
12. Publish draft spec.

13. Have an uplifting spirit.