RDAP Technical Implementation Guide

15 February 2019
Version: 2.1

Contents

I. Introduction

In 2012, The Internet Engineering Task Force (IETF) chartered the WEIRDS (Web Extensible Internet Registration Data Services) working group to replace the WHOIS protocol with a RESTful data service that supports internationalization, a formal data model, and differential services. This working group concluded in early 2015 with the publication of RFC7480, RFC7481, RFC7482, RFC7483, and RFC7484 that define the Registry Data Access Protocol (RDAP) as a standardized replacement for WHOIS. RDAP supports both Regional Internet Registries (RIRs) and Domain Name Registries (DNRs). Since 2015, other RDAP internet drafts and RFCs have been created including RFC8056, draft-ietf-regext-rdap-object-tag, and draft-hollenbeck-regext-rdap-openid, and draft-lozano-rdap-nameservers-sharing-name. The global set of RDAP RFCs and Internet Drafts are referred to as the RDAP Specifications.

The purpose of this document is to provide technical instructions to Domain Name Registries and Registrars on how to implement the Registration Data Access Protocol (RDAP). This document should be used in conjunction with a RDAP Response Profile document.

Additionally, the process of creating these two documents has been memorialized in the RDAP Pilot Working Group Report, which is available for download on the page where this document is hosted. The Report contains important information about the process by which these

specifications were developed including the rationale for certain decisions (both controversial and not), the consideration of public comments, input provided by ICANN Org, items where dissent was registered by participants, and areas for future consideration.

II. Implementation Instruction

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1. RDAP protocol:

1.1. An RDAP server MUST implement the following RFCs or their respective successors:

1.1.1. RFC7480 - HTTP Usage in the Registration Data Access Protocol (RDAP)

1.1.2. RFC7481 -Security Services for the Registration Data Access Protocol (RDAP)

1.1.3. RFC7482 - Registration Data Access Protocol (RDAP) Query Format

1.1.4. RFC7483 - JSON Responses for the Registration Data Access Protocol (RDAP)

1.1.5. RFC7484 - Finding the Authoritative Registration Data (RDAP) Service

1.1.6. RFC8056 - Extensible Provisioning Protocol (EPP) and Registration Data Access Protocol (RDAP) Status Mapping

1.2. The RDAP service MUST be provided over HTTPS only.

1.3. An RDAP server MUST use the best practices for secure use of TLS as described in RFC7525 or its successors.

1.4. An RDAP client SHOULD be able to successfully validate the TLS certificate used for the RDAP service with a *TLSA* record from the DNS (RFC6698 and RFC7671) published by the RDAP service provider. The certificate(s) for the RDAP service associated by DNS-Based Authentication of Named Entities (DANE) SHOULD satisfy the requirements of section 1.5.

1.5. The TLS certificate used for the RDAP service SHOULD be issued by a Certificate Authority (CA) trusted by the major browsers and operating systems

such as the ones listed in the Mozilla Included CA Certificate List (https://wiki.mozilla.org/CA:IncludedCAs). The TLS certificate used for the RDAP service SHOULD be issued by a CA that follows the latest CAB Forum Baseline Requirements (https://cabforum.org/baseline-requirements-documents).

1.6. The RDAP server MUST support both RFC7480 GET and HEAD types of HTTP methods.

1.7. An *rdapConformance* object [RFC7483] MUST be present in the topmost object of every response, and it MUST contain the conformance level of the RDAP protocol and of any extensions, as specified in RFC7483.

1.8. RDAP services MUST be available over both IPv4 and IPv6 transport.

1.9. DNSSEC Requirements:

1.9.1. The resource records for the RDAP service SHOULD be signed with DNSSEC, and if DNSSEC is in place, the DNSSEC chain of trust from the root trust anchor to the name of the RDAP server MUST be valid.

1.10. RDAP servers MUST only use fully qualified domain names in RDAP responses.

1.11. Registry Bootstrap Requirements:

1.11.1. The base URL of Registry RDAP services MUST be registered in the IANA's Bootstrap Service registry for Domain Name Space (https://www.iana.org/assignments/rdap-dns/rdap-dns.xhtml), as described in RFC7484, through the IANA Root Zone Management system. A separate entry is required for each TLD.

1.11.2. When the Registry RDAP service base URL needs to be changed, the previous URL and the new one MUST remain in operation until: 1) the IANA's Bootstrap Service registry for Domain Name Space is updated, and 2) the date and time in the Expires HTTP header of a HTTP/GET request performed on the IANA's Bootstrap registry for Domain Name Space (after the new URL has been published) has elapsed.

1.12. Registrar Bootstrap Requirements

1.12.1. The base URL of Registrar RDAP services MUST be registered in the IANA’s Bootstrap Service registry for registrars, when available. Until such time that the aforementioned registry for registrar RDAP services is

available, the registration MUST be registered with ICANN using the registrar IANA ID as the key.

1.12.2. When the Registrar RDAP service base URL needs to be changed, the previous URL and the new one MUST remain in operation until: 1) the then-current registrar Bootstrap Service registry is updated, and 2) the date and time in the Expires HTTP header of a HTTP/GET request performed on the then-current registrar Bootstrap (after the new URL has been published) has elapsed.

1.13. When responding to RDAP valid requests, an RDAP server MUST include the Access-Control-Allow-Origin response header, as specified by [W3C.REC-cors-20140116]. Unless otherwise specified, a value of "*" MUST be used.

1.14. An RDAP server that conforms to this specification MUST include the string literal "icann_rdap_technical_implementation_guide" as a prefix in the "rdapConformance" member of all responses provided by the server and the suffix of “0”, concatenated according to [RFC7483] section 4.1. For clarity, conformance to the current document MUST be noted with a value of “icann_rdap_technical_implementation_guide_0”. Note: At the time of publication, "icann_rdap_technical_implementation_guide" is pending registration in the IANA RDAP Extensions Registry.

1.15. RDAP extensions

1.15.1. RDAP URI path segment extensions, if used, MUST be registered in the IANA's RDAP Extensions registry (https://www.iana.org/assignments/rdap-extensions/rdap-extensions.xhtml), as defined in RFC7480.

2. RDAP Query Support

2.1. Domain name RDAP queries

2.1.1. The RDAP server MUST support Internationalized Domain Name (IDN) RDAP lookup queries using A-label and U-label format [RFC5890] for domain names.

2.2. Name server RDAP queries. This section applies only to Registries that support the host object model as described in RFC 5731.

2.2.1. The RDAP server MUST support Internationalized Domain Name (IDN) RDAP lookup queries using A-label and U-label format [RFC5890] for name server objects.

2.2.2. RDAP servers MUST support *nameserver* path queries based on the name server name as specified in 3.1.4 of RFC7482.

2.2.3. RDAP servers operated by Registries MUST support *nameserver* search queries based on IP address as defined in RFC7482 section 3.2.2, which, for clarity, does not require pattern matching.

2.2.4. RDAP servers operated by Registries MAY support nameserver search queries based on a "nameserver search pattern" as defined in RFC7482 section 3.2.2.

2.3. Contact object RDAP queries

2.3.1. Contact (object) lookups if supported MUST support RDAP lookup requests for *entities* with any role within other objects using the *handle* (as described in 3.1.5 of RFC7482).

2.4. Registrar object RDAP queries. This section applies only to Registries

2.4.1. Registry RDAP servers MUST support Registrar object lookup using an entity path request for *entities* with the *registrar* role using the *handle* (as described in 3.1.5 of RFC7482) where the *handle* of the *entity* with the *registrar* role is be equal to the IANA Registrar ID.

2.4.2. Registrar object lookup by an entity path request using the *fn* element as a handle (encoded according to RFC 3986) MUST be supported by an RDAP server

3. Responses to RDAP queries:

3.1. An RDAP server that receives a query string (for domain name or name server objects) with a mixture of A-labels and U-labels SHOULD reject the query and return an HTTP 400 "Bad Request" response code with an RDAP error response body that indicates the type of error in the *description* member with an OPTIONAL "lang" (language) attribute. An RDAP server MAY process the query and return a response that contains both the *unicodeName* and the *ldhName* members.

3.2. A registry server RDAP response to a domain query MUST contain a *links* object as defined in [RFC7483] section 4.2., in the topmost JSON object of the response. The *links* object MUST contain the elements *rel:related* and *href* containing the Registrar's RDAP URL of the queried domain object if the Registrar's RDAP URL has been defined .

3.3. Terms of Service

3.3.1. The terms of service of the RDAP service MUST be specified in the *notices* object in the initial JSON object of the response.

3.3.2. The *notices* object MUST contain a *links* object [RFC7483] containing an URL of the RDAP service provider.

3.3.3. The RDAP service provider MUST provide a web page with the terms of service of the RDAP service at the URL contained in the *links* object (2.4.2) which MAY be the same as the terms or service in the *notices* object (2.4.1) or MAY expand upon them.

3.4. RDAP Help queries [RFC7482] MUST be answered and include a *links* member with a URL to a document that provides usage information, policy and other explanatory material.

3.5. Truncated RDAP responses MUST contain a *notices* member describing the reason for the truncation. The *notices* object type MUST be of the form “Response truncated due to {authorization|load|unexplainable reason}”.

3.6. Truncated RDAP objects MUST contain a *remarks* member describing the reason for the truncation. The *remarks* object type MUST be of the form “Result set truncated due to {authorization|load|unexplainable reason}”.

3.7. In the case where the RDAP service provider is querying its database directly, and therefore, using real-time data, the *eventAction* type *last update of RDAP database* MUST show the timestamp of the response to the query.

4. Responses to domain name RDAP queries:

4.1. *Entities* MUST use jCard [RFC7095, 3.3.1.3] structured addresses. If a street address has more than one line, it MUST be structured as an array of strings. Example:

["adr", {}, "text",

["", "", ["123 Main Street", "Suite 3305"],
"Any Town", "CA", "91921-1234", "U.S.A."]]

But if it has a single line or street address, it SHOULD be structured as a simple string. Example:

["adr", {}, "text",
["", "", "123 Main Street",
"Any Town", "CA", "91921-1234", "U.S.A."]]

4.2. If the server responses include roles which are not listed below, such roles MUST be registered at the IANA RDAP JSON Values Registry..

5. Responses to nameserver RDAP queries

This section applies only to Registries

5.1. In the case of a Registry in which name servers are specified as domain attributes, the existence of a name server used as an attribute for an allocated domain name MAY be treated as equivalent to the existence of a host object.

6. Responses to Registrar queries

This section applies only to Registries

6.1. The *entity* with the *registrar* role in the RDAP response MUST contain a *publicIDs* member to identify the IANA Registrar ID from the IANA's Registrar ID registry. The type value of the *publicID* object MUST be equal to IANA Registrar ID.

7. Responses to contact RDAP queries

7.1. In a contact *entity* [RFC7483], phone numbers, if returned as part of a response, MUST be inserted as *tel* properties with a *voice* type parameter, as specified in RFC6350, the vCard Format Specification and its corresponding JSON mapping RFC7095.

7.2. In a contact *entity*, fax numbers, if returned as part of a response, MUST be inserted as *tel* properties with a *fax* type parameter, as specified in RFC6350, the vCard Format Specification and its corresponding JSON mapping RFC7095.

Appendix A: RDAP IETF Standards

RDAP standards are a set of specifications, which together provide a complete RDAP service. Each specification is briefly described below.

RFC7480 - HTTP Usage in the Registration Data Access Protocol (RDAP)
https://tools.ietf.org/html/rfc7480
Describes usage of HTTP transport for RDAP, error messages, RDAP extensions, rate limiting and internationalization with URIs.

RFC7481 - Security Services for the Registration Data Access Protocol (RDAP)
https://tools.ietf.org/html/rfc7481
Covers access control, authentication, authorization, privacy, data confidentiality and RDAP services availability considerations.

RFC7482 - Registration Data Access Protocol (RDAP) Query Format
https://tools.ietf.org/html/rfc7482
Defines the URL patterns for networks, autonomous systems, reverse DNS, name servers, registrars and entities queries. Also covers help requests, search (wildcards) and internationalization in requests.

RFC7483 - JSON Responses for the Registration Data Access Protocol (RDAP)
https://tools.ietf.org/html/rfc7483
Defines JSON object classes for domains, name servers, entities, IP networks and autonomous system numbers. Describe answers to help queries, searches, JSON-embedded error codes and truncated answers.

RFC7484 - Finding the Authoritative Registration Data (RDAP) Service
https://tools.ietf.org/html/rfc7484
Describes a method to find the authoritative server for RDAP data.

W3C.REC=cors-20140116 - Cross-Origin Resource Sharing
https://www.w3.org/TR/2014/REC-cors-20140116/
Defines a mechanism to enable client-side cross-origin requests

Appendix B: Other References

RFC7485 - Inventory and Analysis of WHOIS Registration Objects
https://www.rfc-editor.org/rfc/rfc7485.txt

RFC8056 – Extensible Provisioning Protocol (EPP) and Registration Data Access Protocol (RDAP) Status Mapping
https://tools.ietf.org/html/rfc8056
Describes the mapping of the Extensible Provisioning Protocol (EPP) statuses with the statuses registered for us in the Registration Data Access Protocol (RDAP).

IANA RDAP JSON Values Registry
https://www.iana.org/assignments/rdap-json-values/rdap-json-values.xhtml
This registry defines valid values for RDAP JSON status, role, notices and remarks, event action, and domain variant relation, as defined in RFC7483.

IANA Bootstrap Service Registry for Domain Name Space
https://www.iana.org/assignments/rdap-dns/rdap-dns.xhtml

draft-lozano-rdap-nameservers-sharing-name - Nameserver objects sharing the same name, support for the Registration Data Access Protocol (RDAP)
https://tools.ietf.org/html/draft-lozano-rdap-nameservers-sharing-name
Describes a Registration Data Access Protocol (RDAP) extension that may be used to retrieve the registration information of a particular nameserver object sharing the name with other nameserver objects.

draft-ietf-regext-rdap-object-tag – Registration Data Access Protocol (RDAP) Object Tagging
https://tools.ietf.org/html/draft-ietf-regext-rdap-object-tag
Describes an update to RFC7484 by describing an operational practice that can be used to add structure to RDAP identifiers that makes it possible to identify the authoritative server for additional RDAP queries.

draft-hollenbeck-regext-rdap-openid – Federated Authentication for the Registration Data Access Protocol (RDAP) using OpenID Connect
https://tools.ietf.org/html/draft-hollenbeck-regext-rdap-openid
Describes a federated authentication system for RDAP based on OpenID Connect.

jCard: The JSON Format for vCard
https://tools.ietf.org/html/rfc7095

vCard Format Specification
https://tools.ietf.org/html/rfc6350

EPP Status Code (ICANN)
https://www.icann.org/epp

Draft Final Report from the Expert Working Group on Internationalized Registration Data
https://gnso.icann.org/en/issues/ird/ird-draft-final-10mar15-en.pdf

Study to Evaluate Available Solutions for the Submission and Display of Internationalized Contact Data
https://www.icann.org/en/system/files/files/transform-dnrd-02jun14-en.pdf

Mozilla Included CA Certificate List
https://wiki.mozilla.org/CA:IncludedCAs