RDAP Technical Implementation Guide

31 July 2018
Version: 1.8

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.

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 mobile 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 MUST be signed with DNSSEC, and 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. Bootstrap Requirements:

1.11.1. The base URL of 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 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.

2. Responses to RDAP queries:

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

2.2. An RDAP server that receives a query string with a mixture of A-labels and U-labels SHOULD reject the query.

2.3. An 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* pointing to the Registrar's RDAP URL of the queried domain name object.

2.4. Terms of Service

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

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

2.4.3. 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.

2.5. 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.

2.6. 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}”.

2.7. 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}”.

2.8. 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.

3. Responses to domain name RDAP queries:

3.1. If the domain name is an IDN, the top-level domain object in the RDAP response MUST contain the U-label format of the domain in the *unicodeName* member [RFC7483]. If the domain name is not an IDN, the *unicodeName* member is optional.

3.2. The *status* member [RFC7483] MUST be a valid status type per the IANA's RDAP JSON Values registry (https://www.iana.org/assignments/rdap-json-values/rdap-json-values.xhtml) of status type.

3.3. The *status* member of a domain object in the RDAP response MUST match the EPP status per [RFC8056] as of the updated date of the RDAP response.

3.4. *Entities* MUST use jCard [RFC7095, 3.3.1.3] structured addresses. If a street address has more than one line, it should 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 not as an array, but as a simple string. Example:

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

Do not structured an address like this:

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

The street address should never be an array containing a single string.

3.5. If the server policy supports roles which are not listed below, the server MUST provide a clear mapping of additional roles.

4. Responses to nameserver RDAP queries

4.1. The name server's name MUST be specified in the *ldhName* in A-label format.

4.2. The *unicodeName* member MAY be present in the response to a *nameserver* lookup.

4.3. 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 MUST be treated as equivalent to the existence of a host object.

5. Responses to Registrar queries

5.1. RDAP servers MUST support lookup for *entities* with the *registrar* role within other objects using the *handle* (as described in 3.1.5 of RFC7482). The *handle* of the *entity* with the *registrar* role MUST be equal to IANA Registrar ID. 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.

6. Responses to contact RDAP queries

6.1. In contact *entities* [RFC7483], phone numbers 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.

6.2. In contact *entities*, fax numbers if used, 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.

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