

Registration Protocols Extensions
Internet-Draft
Intended status: Standards Track
Expires: October 11, 2021

M. Loffredo
M. Martinelli
IIT-CNR/Registro.it
April 9, 2021

**Registration Data Access Protocol (RDAP) Reverse search capabilities
draft-ietf-regext-rdap-reverse-search-06**

Abstract

The Registration Data Access Protocol (RDAP) does not include query capabilities to find the list of domains related to a set of entities matching a given search pattern. In the RDAP context, an entity can be associated to any defined object class. Therefore, a reverse search can be applied to other use cases than the classic domain-entity scenario. This document describes RDAP query extensions that allow servers to provide a reverse search feature based on the relationship between any searchable object and the related entities.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on October 11, 2021.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

- [1. Introduction](#) [2](#)
- [1.1. Conventions Used in This Document](#) [3](#)
- [2. RDAP Path Segment Specification](#) [4](#)
- [3. RDAP Conformance](#) [5](#)
- [4. Implementation Considerations](#) [5](#)
- [5. Implementation Status](#) [5](#)
- [5.1. IIT-CNR/Registro.it](#) [6](#)
- [6. IANA Considerations](#) [6](#)
- [7. Privacy Considerations](#) [6](#)
- [8. Security Considerations](#) [7](#)
- [9. Acknowledgements](#) [7](#)
- [10. References](#) [7](#)
- [10.1. Normative References](#) [7](#)
- [10.2. Informative References](#) [9](#)
- [Appendix A. Paradigms to Enforce Access Control on Reverse Search in RDAP](#) [9](#)
- [Appendix B. Change Log](#) [10](#)
- Authors' Addresses [10](#)

1. Introduction

Reverse Whois is a service provided by many web applications that allow users to find domain names owned by an individual or a company starting from the owner's details, such as name and email. Even if it has been considered useful for some legal purposes (e.g. uncovering trademark infringements, detecting cybercrime cases), its availability as a standardized Whois capability has been objected for two main reasons, which now don't seem to conflict with an RDAP implementation.

The first objection has been caused by the potential risks of privacy violation. However, TLDs community is considering a new generation of Registration Directory Services [[ICANN-RDS1](#)] [[ICANN-RDS2](#)] [[ICANN-RA](#)], which provide access to sensitive data under some permissible purposes and according to adequate policies to enforce the requestor accreditation, authentication, authorization, and terms and conditions of data use. It is well known that such security policies are not implemented in Whois [[RFC3912](#)], while they are in RDAP [[RFC7481](#)]. Therefore, RDAP permits a reverse search implementation complying with privacy protection principles.

Another objection to the implementation of a reverse search capability has been connected with its impact on server processing. Since RDAP supports search queries, the impact of both standard and reverse searches is equivalent and can be mitigated by servers adopting ad hoc strategies. Furthermore, the reverse search is almost always performed by specifying an entity role (e.g. registrant, technical contact) and this can contribute to restricting the result set.

Reverse searches, such as finding the list of domain names associated with contacts or nameservers may be useful to registrars as well. Usually, registries adopt out-of-band solutions to provide results to registrars asking for reverse searches on their domains. Possible reasons for such requests are:

- o the loss of synchronization between the registrar database and the registry database;
- o the need for such data to perform massive EPP [[RFC5730](#)] updates (e.g. changing the contacts of a set of domains, etc.).

Currently, RDAP does not provide any way for a client to search for the collection of domains associated with an entity [[RFC7482](#)]. A query (lookup or search) on domains can return the array of entities related to a domain with different roles (registrant, registrar, administrative, technical, reseller, etc.), but the reverse operation is not allowed. Only reverse searches to find the collection of domains related to a nameserver (ldhName or ip) can be requested. Since an entity can be in relationship with any RDAP object [[RFC7483](#)], the availability of a reverse search can be common to all resource type path segments defined for search.

The protocol described in this specification aims to extend the RDAP query capabilities to enable the reverse search based on the relationship between any object and the associated entities. The extension is implemented by adding new path segments (i.e. search paths) and using a RESTful web service [[REST](#)]. The service is implemented using the Hypertext Transfer Protocol (HTTP) [[RFC7230](#)] and the conventions described in [[RFC7480](#)].

1.1. Conventions Used in This Document

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.

2. RDAP Path Segment Specification

The new search paths are OPTIONAL extensions of those defined in [\[RFC7482\]](#). A generic reverse search path is described by the syntax:

```
{resource-type}/reverse/{role}?{property}=<search pattern>
```

The path segments are defined as in the following:

- o resource-type: it MUST be one of resource type path segments defined in [Section 3.2 of \[RFC7482\]](#): "domains", "nameservers" or "entities";
- o role: it MUST be one of the roles described in [Section 10.2.4 of \[RFC7483\]](#). For role independent reverse searches, the value "entity" MUST be used;
- o property: it identifies the entity property to be used in matching the search pattern. A pre-defined list of properties includes: fn, handle, email, city, country, cc. The mapping between such properties and the RDAP properties is shown in Table 1. Some of the properties are related to jCard elements [\[RFC7095\]](#) but, being jCard the JSON format for vCard [\[RFC6350\]](#), the corresponding definitions are included in vCard specification. Servers MAY implement additional properties to those defined in this document.

Partial string matching is allowed as defined in [section 4.1 of \[RFC7482\]](#).

Reverse search property	RDAP property	RFC 7483	RFC 6350	RFC 8605
handle	handle	5.1.		
fn	jCard fn		6.2.1	
email	jCard email		6.4.2	
city	locality in jCard		6.3.1	
	adr			
country	country name in jCard adr		6.3.1	
	jCard adr			
cc	country code in jCard adr			3.1

Table 1: Mapping between the reverse search properties and the RDAP properties


```
https://example.com/rdap/domains/reverse/technical?handle=CID-40*  
https://example.com/rdap/domains/reverse/registrant?fn=Bobby*  
https://example.com/rdap/domains/reverse/registrant?cc=US  
https://example.com/rdap/entities/reverse/registrant?handle=RegistrarX
```

Figure 1: Examples of reverse search queries

The "country" property can be used as an alternative to "cc" when RDAP servers don't include the jCard "cc" parameter [[RFC8605](#)] in their response.

3. RDAP Conformance

Servers complying with this specification MUST include the value "reverse_search" in the rdapConformance property of the help response [[RFC7483](#)]. The information needed to register this value in the "RDAP Extensions" registry is described in [Section 6](#).

4. Implementation Considerations

The implementation of the proposed extension is technically feasible. Both handle and fn are used as standard path segments to search for entities [[RFC7482](#)]. With regards to the other reverse search properties, namely email, city and country code, the impact of their usage on server processing is evaluated to be the same as other existing query capabilities (e.g. wildcard prefixed search pattern) so the risks to degrade the performance or to generate huge result sets can be mitigated by adopting the same policies (e.g. restricting the search functionality, limiting the rate of search requests according to the user profile, truncating and paging the results, returning partial responses).

5. Implementation Status

NOTE: Please remove this section and the reference to [RFC 7942](#) prior to publication as an RFC.

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in [[RFC7942](#)]. The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was

supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations may exist.

According to [RFC 7942](#), "this will allow reviewers and working groups to assign due consideration to documents that have the benefit of running code, which may serve as evidence of valuable experimentation and feedback that have made the implemented protocols more mature. It is up to the individual working groups to use this information as they see fit".

5.1. IIT-CNR/Registro.it

Responsible Organization: Institute of Informatics and Telematics of National Research Council (IIT-CNR)/Registro.it

Location: <https://rdap.pubtest.nic.it/>

Description: This implementation includes support for RDAP queries using data from the public test environment of .it ccTLD.

Level of Maturity: This is an "alpha" test implementation.

Coverage: This implementation includes all of the features described in this specification.

Contact Information: Mario Loffredo, mario.loffredo@iit.cnr.it

6. IANA Considerations

IANA is requested to register the following value in the RDAP Extensions Registry:

Extension identifier: reverse_search

Registry operator: Any

Published specification: This document.

Contact: IETF <iesg@ietf.org>

Intended usage: This extension describes reverse search query patterns for RDAP.

7. Privacy Considerations

The use of the capability described in this document MUST be compliant with the rules about privacy protection each RDAP provider is subject to. Sensitive registration data MUST be protected and accessible for permissible purposes only. This functionality SHOULD be only accessible to authorized users and only for a specified use case.

Already the request for this functionality could contain Personal Identifiable Information and SHOULD therefore only be available over HTTPS.

Providing reverse search in RDAP carries the following threats as described in [[RFC6973](#)]:

- o Correlation
- o Disclosure
- o Misuse of information

Therefore, RDAP providers are REQUIRED to mitigate the risk of those threats by implementing appropriate measures supported by security services (see [Section 8](#)).

8. Security Considerations

Security services required to provide controlled access to the operations specified in this document are described in [[RFC7481](#)]. A non exhaustive list of access control paradigms an RDAP provider can implement is presented in [Appendix A](#).

The specification of the entity role within the reverse search path allows the RDAP servers to implement different authorization policies on a per-role basis.

9. Acknowledgements

The authors would like to acknowledge the following individuals for their contributions to this document: Tom Harrison, Scott Hollenbeck, Francisco Arias, Gustavo Lozano, Eduardo Alvarez and Ulrich Wisser.

10. References

10.1. Normative References

- [OIDCC] OpenID Foundation, "OpenID Connect Core incorporating errata set 1", November 2014, <http://openid.net/specs/openid-connect-core-1_0.html>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC3912] Daigle, L., "WHOIS Protocol Specification", [RFC 3912](#), DOI 10.17487/RFC3912, September 2004, <<https://www.rfc-editor.org/info/rfc3912>>.
- [RFC5730] Hollenbeck, S., "Extensible Provisioning Protocol (EPP)", STD 69, [RFC 5730](#), DOI 10.17487/RFC5730, August 2009, <<https://www.rfc-editor.org/info/rfc5730>>.

- [RFC6350] Perreault, S., "vCard Format Specification", [RFC 6350](#), DOI 10.17487/RFC6350, August 2011, <<https://www.rfc-editor.org/info/rfc6350>>.
- [RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", [RFC 6973](#), DOI 10.17487/RFC6973, July 2013, <<https://www.rfc-editor.org/info/rfc6973>>.
- [RFC7095] Kewisch, P., "jCard: The JSON Format for vCard", [RFC 7095](#), DOI 10.17487/RFC7095, January 2014, <<https://www.rfc-editor.org/info/rfc7095>>.
- [RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", [RFC 7230](#), DOI 10.17487/RFC7230, June 2014, <<https://www.rfc-editor.org/info/rfc7230>>.
- [RFC7480] Newton, A., Ellacott, B., and N. Kong, "HTTP Usage in the Registration Data Access Protocol (RDAP)", STD 95, [RFC 7480](#), DOI 10.17487/RFC7480, March 2015, <<https://www.rfc-editor.org/info/rfc7480>>.
- [RFC7481] Hollenbeck, S. and N. Kong, "Security Services for the Registration Data Access Protocol (RDAP)", STD 95, [RFC 7481](#), DOI 10.17487/RFC7481, March 2015, <<https://www.rfc-editor.org/info/rfc7481>>.
- [RFC7482] Newton, A. and S. Hollenbeck, "Registration Data Access Protocol (RDAP) Query Format", [RFC 7482](#), DOI 10.17487/RFC7482, March 2015, <<https://www.rfc-editor.org/info/rfc7482>>.
- [RFC7483] Newton, A. and S. Hollenbeck, "JSON Responses for the Registration Data Access Protocol (RDAP)", [RFC 7483](#), DOI 10.17487/RFC7483, March 2015, <<https://www.rfc-editor.org/info/rfc7483>>.
- [RFC7942] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", [BCP 205](#), [RFC 7942](#), DOI 10.17487/RFC7942, July 2016, <<https://www.rfc-editor.org/info/rfc7942>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.

[RFC8605] Hollenbeck, S. and R. Carney, "vCard Format Extensions: ICANN Extensions for the Registration Data Access Protocol (RDAP)", [RFC 8605](#), DOI 10.17487/RFC8605, May 2019, <<https://www.rfc-editor.org/info/rfc8605>>.

10.2. Informative References

[[draft-ietf-regext-rdap-openid](#)]

Hollenbeck, S., "Federated Authentication for the Registration Data Access Protocol (RDAP) using OpenID Connect", <<https://datatracker.ietf.org/doc/draft-ietf-regext-rdap-openid/>>.

[ICANN-RA]

Internet Corporation For Assigned Names and Numbers, "Registry Agreement", July 2017, <<https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf>>.

[ICANN-RDS1]

Internet Corporation For Assigned Names and Numbers, "Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS)", June 2014, <<https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf>>.

[ICANN-RDS2]

Internet Corporation For Assigned Names and Numbers, "Final Issue Report on a Next-Generation gTLD RDS to Replace WHOIS", October 2015, <<http://whois.icann.org/sites/default/files/files/final-issue-report-next-generation-rds-07oct15-en.pdf>>.

[REST]

Fielding, R., "Architectural Styles and the Design of Network-based Software Architectures", 2000, <http://www.ics.uci.edu/~fielding/pubs/dissertation/fielding_dissertation.pdf>.

Appendix A. Paradigms to Enforce Access Control on Reverse Search in RDAP

Access control can be implemented according to different paradigms introducing increasingly stringent rules. The paradigms reported here in the following leverage the capabilities either supported natively or provided as extensions by the OpenID Connect [[OIDCC](#)]:

- o Role-Based Access Control: access rights are granted depending on roles. Generally, this is done by grouping users into fixed categories and assigning each category with static grants. A more dynamic approach can be implemented by using the OpenID Connect "scope" claim;
- o Purpose-Based Access Control: access rules are based on the notion of purpose which means the intended usage of some data by a user. It can be implemented by tagging a request with the usage purpose and making the RDAP server check the compliance between the given purpose and the control rules applied to data to be returned. The purpose can be stated within an out-of-band process by setting the OpenID Connect RDAP specific "purpose" claim as defined in [\[draft-ietf-regext-rdap-openid\]](#);
- o Attribute-Based Access Control: rules to manage access rights are evaluated and applied according to specific attributes describing the context within which data are requested. It can be implemented by setting within an out-of-band process additional OpenID Connect claims describing the request context and making the RDAP server check the compliance between the given context and the control rules applied to data to be returned;
- o Time-Based Access Control: data access is allowed for limited time only. It can be implemented by assigning the users with temporary credentials linked to access grants whose scope is limited.

[Appendix B](#). Change Log

- 00: Initial working group version ported from [draft-loffredo-regext-rdap-reverse-search-04](#)
- 01: Updated "Privacy Considerations" section.
- 02: Revised the text.
- 03: Refactored the query model.
- 04: Keepalive refresh.
- 05: Reorganized "Abstract". Corrected "Conventions Used in This Document" section. Added "RDAP Conformance" section. Changed "IANA Considerations" section. Added references to [RFC7095](#) and [RFC8174](#). Other minor edits.
- 06: Updated "Privacy Considerations", "Security Considerations" and "Acknowledgements" sections. Added some normative and informative references. Added [Appendix A](#).

Authors' Addresses

Mario Loffredo
IIT-CNR/Registro.it
Via Moruzzi,1
Pisa 56124
IT

Email: mario.loffredo@iit.cnr.it
URI: <http://www.iit.cnr.it>

Maurizio Martinelli
IIT-CNR/Registro.it
Via Moruzzi,1
Pisa 56124
IT

Email: maurizio.martinelli@iit.cnr.it
URI: <http://www.iit.cnr.it>

