Network Working Group
Internet-Draft
Expires: January 25, 2004

V. Listman, Editor
American Registry for Internet Numbers

July 25, 2003

Cross Registry Internet Service Protocol (CRISP) Internet Resource Number Requirements

draft-ietf-crisp-internet-resource-number-req-00

Status of this Memo

Copyright Notice

Abstract

Internet registries expose administrative and operational data via varying directory services. This document defines functional requirements for the directory services of Internet resource number registries.

Table of Contents

1. Introduction

1.1 Background

The expansion and growth of the Internet has seen the registry function of a traditionally centralized and managed Network Information Center become the responsibility of various autonomous, functionally disparate, and globally distributed Internet registries. With the broadening number of Internet registries, the uses of their administrative directory services have expanded from the original and traditional use of the whois [5] protocol to include the use of whois outside the scope of its specification, formal and informal definitions of syntax, undocumented security mechanisms, the use of other protocols, such as rwhois [4], to fulfill other needs, and proposals for the use of other technologies such as LDAP [3] and XML.

1.2 Requirements Scope

The scope of the requirements captured in this document relate to the directory services of Internet resource number registries and their related communities (Section 2.1 and Section 2.2). Additional communities are described in the Cross Registry Internet Service Protocol (CRISP) Requirements draft [6]. These requirements are not specific to any protocol. Terms used in the definition of the requirements in this document may be found in the glossary (Appendix A).

The scope of the requirements in this document is also restricted to access of data from Internet registries. Requirements for modification, addition, or provisioning of data in Internet registries are out of scope.

1.3 Requirements Specification

The requirements captured in this document are for the purpose of designing technical specifications. The words used in this document for compliance with RFC2119 [2] do not reference or specify policy and speak only to the capabilities in the derived technology. For instance, this document may say that the protocol "MUST" support certain features. An actual service operator is always free to disable it (and then to return an error such as "permission denied".)

Requirements in this document specifying the capabilities of the protocol required for proper interaction between a client and a server will be specified with the "MUST/SHOULD" language of RFC2119 [2]. This document also contains language relating to the interaction of a client with multiple servers to form a coherent, cross-network service. Such service requirements will not be described using RFC2119 language.

While individual servers/service operators may not support all features that the protocol can support, they must respect the semantics of the protocol queries and responses. For example, a server should not return referrals if it does not have referent data.

2. Internet Registry Communities

The Internet registries are composed of various communities which provide scope for the requirements in this document. This document describes those communities specifically involved with Internet resource number registration. Other communities are described in the Cross Registry Internet Service Protocol (CRISP) Requirements draft [6]. These descriptions are provided in this document for informational purposes only.

2.1 Regional Internet Registries

Regional Internet Registries (RIRs) administer the allocation of IP address space and autonomous system numbers. Each RIR serves specific geographic regions, and collectively they service the entire Internet. Each RIR is a membership-based, non-profit organization that facilitates and implements addressing policy based on the direction of their regional community.

2.2 Other Internet Registries

Local Internet Registries (LIRs), National Internet Registries (NIRs) and Internet Service Providers (ISPs) are registries of the RIRs and coordinate the same functions of the RIRs for smaller, more specific geographic regions, sovereign nations, localities, and business regions.

3. Functional Requirements

Functional requirements describe an overall need or process for which the directory service is used by an Internet registry to fulfill its obligations to provide information about their customers, members and the resources they hold. This section describes requirements in the manner specified in Section 1.3.

3.1 Base Functions

This section describes basic directory service protocol requirements for Internet registries. Additional requirements, specific to Internet resource number registries, are described in Internet Resource Number Specific Functions (Section 3.2).

3.1.1 Mining Prevention

In order to prevent the inappropriate acquisition of data from an Internet registry's directory service, servers may limit the amount of data that may be returned in a fixed time period from a server to a client. This will most likely be especially true for anonymous access uses (see Section 3.1.4).

The limits placed on differing types of data or applied depending upon access status will most likely differ from server to server based on policy and need. Support for varying service models in the effort to limit data and prevent data mining may or may not have a direct impact on the client-to-server protocol, but MUST NOT be prevented by the protocol.

3.1.2 Minimal Technical Reinvention

The protocol MUST NOT employ unique technology solutions for all aspects and layers above the network and transport layers and SHOULD make use of existing technology standards where applicable. The protocol MUST employ the use of network and transport layer standards as defined by the Internet Engineering Task Force. The protocol MUST define one or more transport mechanisms for mandatory implementation.

3.1.3 Standard and Extensible Schemas

3.1.3.1 Protocol Requirement

The protocol MUST contain standard schemas for the exchange of data needed to implement the functionality in this document. In addition, there MUST be a means to allow the use of schemas not defined by the needs of this document. Both types of schemas MUST use the same schema language. The schemas MUST be able to express data elements with identifying tags for the purpose of localization of the meaning

of the identifying tags.

3.1.3.2 Service Description

The client-to-server protocol must define a standard set of data structures or schemas to be used when exchanging information. It must also possess the ability to allow for the use of newer data structures that are currently nor foreseen by this specification. In both cases, the description and specification of both types of data structures or schemas must be done in the same way (i.e. the same schema language).

The schemas must also be capable of "tagging" data with a unique identifier. This identifier can then be used to localize the name of that type of data. For instance, a piece of data may have the value "Bob" and its type identified with the number "5.1". Client software could use this to display "Name: Bob" in an English locale or "Nombre: Bob" in a Spanish locale.

3.1.4 Level of Access

3.1.4.1 Protocol Requirement

The protocol MUST NOT prohibit an operator from granularly assigning multiple types of access to data according to the policies of the operator. The protocol MUST provide an authentication mechanism and MUST NOT prohibit an operator from granting types of access based on authentication.

The protocol MUST provide an anonymous access mechanism that may be turned on or off based on the policy of an operator.

3.1.4.2 Service Description

Server operators may offer varying degrees of access depending on policy and need. The following are some examples:

- users may be allowed access only to data for which they have a relationship
- unauthenticated or anonymous access status may not yield any contact information
- full access may be granted to a special group of authenticated users

The types of access allowed by a server will most likely vary from one operator to the next.

3.1.5 Client Processing

The protocol MUST be capable of allowing machine parsable requests

and responses.

3.1.6 Entity Referencing

There MUST be a mechanism for an entity contained within a server to be referenced uniquely by an entry in another server.

3.1.7 Decentralization

3.1.7.1 Protocol Requirement

The protocol MUST NOT require the aggregation of data to a central repository, server, or entity. The protocol MUST NOT require aggregation of data indexes or hints to a central repository, server, or entity.

3.1.7.2 Service Description

Some server operators may have a need to coordinate service in a mesh or some other framework with other server operators. However, the ability to operate a CRISP compliant server must not require this.

3.1.8 Authentication Distribution

3.1.8.1 Protocol Requirement

The protocol MUST NOT require any Internet registry to participate in any authentication system. The protocol MUST NOT prohibit the participation by an Internet registry in federated, distributed authentication systems.

3.1.8.2 Service Description

Some server operators may have a need to delegate authentication to another party or participate in a system where authentication information is distributed. However, the ability to operate a CRISP compliant server must not require this.

3.1.9 Base Error Responses

The protocol MUST be capable of returning the following types of non-result or error responses to all lookups and searches:

- permission denied - a response indicating that the search or lookup has failed due to insufficient authorization.
- not found - the desired results do not exist.
- insufficient resources - the search or lookup requires resources

that cannot be allocated.

3.1.10 Query Distribution

3.1.10.1 Protocol Requirement

The protocol MUST NOT prohibit a server from participating in a query distribution system.

3.1.10.2 Service Description

For lookups and searches requiring distribution of queries, the client must be allowed to distribute these queries among the participants in an established mesh of server operators. It is not a requirement that the protocol enable the discovery of servers, but cooperating servers should be able to intelligently handle distribution with its established mesh. Individual server operators will respond to all queries received according to their policies for authentication, privacy, and performance.

However, the ability to operate a CRISP compliant server must not require the participation in any query distribution system.

3.1.11 Protocol and Schema Versioning

3.1.11.1 Protocol Requirements

The protocol MUST provide a means by which the end-systems can either identify or negotiate over the protocol version to be used for any query or set of queries.

All resource-specific schemas MUST provide version identifier attributes which uniquely and unambiguously identifies the version of the schema being returned in the answer set to a query.

3.1.11.2 Service Description

The service should allow end-systems using different protocol versions to fallback to a mutually supported protocol version. If this is not possible, the service must provide a meaningful error which indicates that this is the specific case.

The service must suggest negotiation and/or recovery mechanisms for clients to use when an unknown schema version is received.

3.2 Internet Resource Number Specific Functions

These functions describe requirements specifically needed by Regional Internet Registries (Section 2.1). No compliant server operator is required to support the functions required by every registry type.

3.2.1 Lookups

Lookups are queries by unique identifiers resulting in zero or one match.

3.2.1.1 Protocol Requirement

The protocol MUST be able to query for information relating to the following kinds of objects:

1. IPv4 network address(es)

2. IPv6 network address(es)

3. Autonomous system number(s)

4. Contact

5. Organization

See Section 3.2.3 for the requirements regarding the expected return values.

3.2.1.2 Service Description

These lookups are all single index queries, have a unique identifier and should produce zero or only one entity.

Depending on the policy and need of an Internet registry, a server operator may not allow all or any of these lookups to return part or all of the information. See Section 3.2.3.

3.2.2 Searches

Searches are queries by attributes that may not be unique resulting in zero, one or many matches.

3.2.2.1 Protocol Requirement

The protocol MUST contain the following search functions:

1. IPv4 address search given one or more contiguous IP address numbers. This search SHOULD allow for both exact matching and nested matching.

2. IPv6 address search given one or more contiguous IP address numbers. This search SHOULD allow for both exact matching and nested matching.

3. Autonomous system number search given one or more contiguous numbers. This search SHOULD allow for both exact matching and

nested matching.

4. Contact search by either exact name or partial name matching.

5. Organization search by either exact name or partial name matching.

See Section 3.2.3 for the requirements regarding the expected return values.

3.2.2.2 Service Description

These searches may be multi-index queries and may produce zero, one or many entities.

Depending on the policy and need of an Internet registry, a server operator may not allow all or any of these searches to return part or all of the information. See Section 3.1.4. Access to information resulting from these searches may also be limited, depending on policy, by quantity. Section 3.2.5 describes these types of restrictions.

Some Internet registries may also be participating in a query distribution system. See Section 3.1.10.

3.2.3 Information Sets

3.2.3.1 Protocol Requirements

The data sets for networks, autonomous systems, contacts, and organizations MUST be able to express and represent the attributes and allowable values of registered Internet resource number registration and provisioning protocols.

The data set for networks, autonomous systems, organizations and contacts MUST be able to express arbitrary textual information for extensions on an individual operator basis. Examples of such information are authorized use policies, extended status notifications, marketing/for sale notices, and URI references to other sources.

3.2.3.1.1 IP Address Network Return Values

The schema MUST be capable of expressing the following information for IP address networks:

- range of IP addresses
- network type, for example, allocated or assigned
- contacts and the function/role served

- organization holding the address space

- reverse delegation information
- last updated date
- registry delegating the address space

3.2.3.1.2 Autonomous System Return Values

The schema MUST be capable of expressing the following information for autonomous systems:

- range of autonomous system number(s)
- contacts and function/role served
- organization holding the resource
- last updated date
- registry delegating the resource

3.2.3.1.3 Contact Return Values

The schema MUST be capable of expressing the following information for contacts:

- name of contact
- unique identifier
- postal address including country code
- telephone number(s), extension(s), and type
- e-mail address(es)
- last updated date

3.2.3.1.4 Organization Return Values

The schema MUST be capable of expressing the following information for organizations:

- name of organization
- unique identifier
- postal address including country code
- contacts and function/role served

- last updated date

3.2.3.2 Service Description

It is not expected that every Internet registry supply all of the information spelled out above, however the schemas employed by the protocol must be capable of expressing this information should a registry need to provide it.

The following sections describe requirements relative to the use of schemas with respect to individual registry need and policy:

- Section 3.2.6
- Section 3.2.4
- Section 3.1.4
- Section 3.1.1

3.2.4 Result Set Limits

3.2.4.1 Protocol Requirement

The protocol MUST contain a feature, used at the discretion of a server operator, to allow a server to express to a client a limit on the number of results from searches and lookups. When returning result sets, the protocol MUST be able to make the following distinctions:

1. an empty result set.
2. a result set truncated for the purpose of improving performance bottlenecks.
3. a result set truncated to comply with Section 3.1.1

3.2.4.2 Service Description

Client software will operate more usefully if it can understand reasons for the truncation of result sets. Of course, some Internet registries may not be able to expose their policies for the limiting of result sets, but, when it is possible, clients will have a better operational view. This may eliminate re-queries and other repeated actions that are not desirable.

3.2.5 Distribution for Internet Resource Number Registry Types

3.2.5.1 Protocol Requirement

The protocol MUST NOT prohibit the distribution of data to exclude

any of the registry types stated in Section 2. The protocol MUST be capable of expressing referrals and entity references between the various registry types described in Section 2.

3.2.5.2 Service Description

An RIR will allocate IP address space to those registration entities described in Section 2.2. These entities may be given the option to store utilization within the RIR database, or establish their own server to be referenced as needed. If the entity establishes their own server, it must comple with the requirements of this document.

3.2.6 Data Omission

3.2.6.1 Protocol Requirement

When a value in an answer to a query cannot be given due to policy constraints, the protocol MUST be capable of expressing the value in one of three ways:

1. complete omission of the value without explanation

2. an indication that the value cannot be given due to insufficient authorization

3. an indication that the value cannot be given due to privacy constraints regardless of authorization status

The protocol MAY define other values for this purpose, but MUST define values defined above at a minimum.

3.2.6.2 Service Description

Internet registries will have varying constraints regarding their ability to expose certain types of data. Server operators must have the ability to accommodate this need while client software will be more useful when provided with proper explanations. Therefore, depending on policy, a server operator has a choice between not returning the data at all, signaling a permission error, or indicating a privacy constraint.

3.2.7 Internationalization

The schema defining Internet number related resources MUST conform to RFC 2277 [1] regarding textual data. In particular, the schema MUST be able to indicate the charset and language in use with unstructured textual data.

The protocol MAY be able to support multiple representations of

contact data, with these representations complying with the

requirements in Section 3.2.3. The protocol MUST be able to provide contact data in UTF-8 and SHOULD be able to provide contact data in US-ASCII, other character sets, and capable of specifying the language of the data.

3.2.8 Privacy

The following sections describe requirements related to the privacy of the data stored in the database:

- Section 3.1.4
- Section 3.1.1

4. Feature Requirements

Feature requirements describe the perceived need derived from the functional requirements for specific technical criteria of the directory service. This section describes requirements in the manner specified in Section 1.3.

4.1 Client Authentication

Entities accessing the service (users) MUST be provided a mechanism for passing credentials to a server for the purpose of authentication. The protocol MUST provide a mechanism capable of employing many authentication types and capable of extension for future authentication types.

4.2 Referrals

To distribute queries for search continuations and to issue entity references, the protocol MUST provide a referral mechanism.

4.3 Common Referral Mechanism

To distribute queries for search continuations and to issue entity references, the protocol MUST define a common referral scheme and syntax.

4.4 Structured Queries and Responses

To provide for machine consumption as well as human consumption, the protocol MUST employ structured queries and responses.

5. Internationalization Considerations

Requirements defined in this document MUST consider the best practices spelled out in [1].

6. IANA Considerations

IANA consideration for any service meeting these requirements will depend upon the technologies chosen and MUST be specified by any document describing such a service.

7. Security Considerations

This document contains requirements for the validation of authenticated entities and the access of authenticated entities compared with the access of non-authenticated entities. This document does not define the mechanism for validation of authenticated entities. Requirements defined in this document MUST allow for the implementation of this mechanism according best common practices.

The requirement in Section 3.1.4 must be weighed against other requirements specifying search or lookup capabilities.

This document contains requirements for referrals and entity references. Client implementations based on these requirements SHOULD take proper care in the safe-guarding of credential information when resolving referrals or entity references according to best common practices.

This document contains requirements for the distribution of queries among a mesh of participating service providers. Protocols proposed to meet these requirements must be able to protect against the use of that distribution system as a vector of distributed denial of service attacks or unauthorized data mining.

Normative References

[1] Alvestrand, H., "IETF Policy on Character Sets and Languages", BCP 18, RFC 2277, January 1998.

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

Informative References

[3] Wahl, M., Howes, T. and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

[4] Williamson, S., Kosters, M., Blacka, D., Singh, J. and K. Zeilstra, "Referral Whois (RWhois) Protocol V1.5", RFC 2167, June 1997.

[5] Harrenstien, K., Stahl, M. and E. Feinler, "NICNAME/WHOIS", RFC 954, October 1985.

[6] Newton, A., "Cross Registry Internet Service Protocol (CRISP) Requirements", draft-ietf-crisp-requirements-05, May 2003.

Editor's Address

Virginia Listman
American Registry for Internet Numbers
3635 Concorde Parkway, Suite 200
Chantilly, VA 20151
USA

Phone: +1 703 227 9870
EMail: ginny@arin.net

Appendix A. Glossary

- contact data: Data containing names and contact information (i.e. postal addresses, phone numbers, e-mail addresses) of humans or legal entities.

- operational data: Data necessary to the operation of networks and network related services and items.

- RIR: Initials for "regional Internet registry."

- mining: In the context of this document, this term is specific to data mining. This is a methodical process to obtain the contents of directory service, usually as much as possible, not relevant to any immediate operational Internet need. Data mining is often not a practice welcomed by registry operators.

Appendix B. Acknowledgements

B.1 Working Group

This document is a work item of the Cross-Registry Internet Service Protocol (CRISP) Working Group in the Applications Area of the IETF. Discussions for this working group are held on the email list ietf-not43@lists.verisignlabs.com. To subscribe to this email list, send email to ietf-not43-request@lists.verisignlabs.com with a subject line of "subscribe". Archives of this list may be found out http://lists.verisignlabs.com/pipermail/ietf-not43/.

B.2 Contributions

The contents of this document are the compiled requirements of the four existing Regional Internet Registries: Asia Pacific Network Information Centre (APNIC), the American Registry for Internet Numbers (ARIN), the Latin American and Caribbean Internet Address Registry (LACNIC) and Reseaux IP Europeens Network Coordination Centre (RIPE NCC).

Specific comments, suggestions, and feedback of significant substance have been provided by Tim Christensen, Shane Kerr, George Michaelson, Cathy Murphy and Frederico Neves.

Intellectual Property Statement

Full Copyright Statement

MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.