Overview

As detailed in Specification 4 “Specification for Registration Data Publication Services” (RDPS), the Registry Operator will operate a fully compliant “Registration Data Directory Service” (RDDS), will provide “Zone File Access” as required and will grant ICANN the required “Bulk Registration Data Access”. These services will fulfil the requirements stated in the respective specification, and will also meet or exceed the respective RDDS SLAs as required in Specification 10.

In addition to the requisite WHOIS service, a lightweight variant of the RDDS, a so-called “Domain Availability Interface”, based on the “finger” protocol, will be provided. This service will supplement the WHOIS service, and exposes a very limited subset of the information already available via the RDDS, namely, whether or not a certain domain name is available for registration.

1 Registration Data Directory Services

A WHOIS service will be available via port 43 in compliance with RFC 3912. Additionally a web-based directory service, to be made available at “whois.nic.versicherung”, will provide a free, publicly accessible, query-based interface which will provide information regarding “Domain Name”, “Registrar” and “Nameserver” objects. The data format used for those objects is specified below. It is understood that ICANN reserves the right to require alternative formats and protocols, and upon such specification, such changes will be implemented as soon as reasonably practicable.

Specifically, the WHOIS service fulfils the following requirements:

- The server is fully compliant with RFC 3912
- Free public query-based access is provided
- The services runs on “whois.nic.versicherung” on TCP port 43
- Data objects represented by key/value pairs, with multiple key/value pairs with the same key in case of fields with more than one value
- Additionally, web-based access on “whois.nic.versicherung” is provided
- In order to prevent abuse, highly configurable volume access limitations are deployed
- The architecture is robust, implements a number of failsafe mechanisms and is in compliance with the RDDS SLA’s outlined in Specification 10.

1.1 Architecture

The technical architecture of the WHOIS system (servers, switches, routers, etc.) is depicted in Figure Q26-02, and employs the following components:

- Connectivity to the internet is handled via the two redundant access routers of the registry system. Each server is connected to each of the two routers, with one connection serving as an active path, and the second path (to the other router) serving as a failover path in case of failure of the first.
- Two virtual machines on physically separate hardware run the frontend Whois/Finger/HTTP daemons.

- The WHOIS service on each server operates as part of an active-active cluster. Both servers announce their respective service addresses to the routers via OSPF with the routers distributing traffic between the two frontends by means of OSPF load sharing logic.
- Both active instances are connected to the active registry database using persistent database connections to reduce session handling overhead. The frontend servers switch automatically to the registry standby database in the event of a database failover.
- In the case where one of the frontend servers fails, the OSPF announcement for that server automatically ceases and traffic is redirected to the remaining active node within a few seconds.
- Access is restricted to TCP port 43 (for Whois), TCP port 79 (for Finger) and TCP port 80 (HTTP) using firewall access lists on the routers.
- The codebase for the WHOIS and Finger servers was developed in-house using the "C" programming language and is based on state-of-the art design concepts to ensure a robust and stable operation. This software has been actively developed for a number of years and is currently in production at the ".at" and ".no" TLD registries.
- The software is also highly configurable, allowing query limits to be set based on source IP address/blocks for both IPv6 and IPv4 addressing formats. It also allows for fine grained control of specific rate-limits on a per network block basis.
- The software actively generates access and service statistics for monitoring and management purposes.
- The RDDS uses the "live" registry database and as a result updates to the registry database are reflected in real-time to the WHOIS server. However, in the event that the WHOIS load starts to impact the performance of the Registry database, provisions are in place to move the WHOIS server to an alternate read-only replica of the "live" database if necessary.

1.2 Access Limitations and Access Restrictions

Access control lists (ACLs) protect the RDDS service hosts against unwanted access but grant public access to the defined services (WHOIS, finger, HTTP).

In addition to this general protection of the service infrastructure, the RDDS must also make provision to address the following scenarios:

- Bulk requests from public unknown sources (e.g. to grab data)
- High speed / high volume requests from known source addresses (e.g. from registrars)

In order to handle the above scenarios the WHOIS software supports the following configurable service policies:

- The number of allowed requests (within a specific time frame) on a per IP address (or per IP subnet) basis, for either IPv4 or IPv6 and with support for a "most specific" matching rule of those entries. This provides the ability to set different limitations for different user groups / network ranges. Violations of those limits are included in the daily WHOIS service reports sent to the operations team.

1.3 WHOIS Input Format

The data format complies with the requirements of Specification 4 of the “new gTLD agreement”. The definitions below apply to the command line WHOIS interface (port 43) as well as the web interface:

- Queries can be issued for domain name, registrar and nameserver objects
- Queries that include the argument “registrar” trigger a search for registrar data objects. If the argument is “nameserver”, a search for nameserver objects is actioned, while queries without any such prefix trigger a search for a domain or nameserver.
- Wildcard searches and substring searches are not supported.
- Using the option “-C” (“charset”) as part of the command line WHOIS query specifies a character encoding for the protocol. This setting applies to the both the input and output character encoding, and supports the following values: “US-ASCII”, “ISO-8859-1” and “UTF-8”. The default character set is “UTF-8”. On the web interface the character encoding will always be set to UTF-8 with modification of this option not available.
- In the case of IDNs, the search string must be in the A-Label format of the domain or nameserver. Searches based on the U-Label format are not supported.

Example queries (including the command line “whois” client itself):

- Domain name data: whois -h whois.nic.versicherung example.versicherung
- Domain name data (with character set parameter): whois -h whois.nic.versicherung -- -C us-ascii example.versicherung
- Registrar data: whois -h whois.nic.versicherung “registrar Example Company”
- Nameserver data by name: whois -h whois.nic.versicherung ns1.example.tld
- Nameserver data by IP address: whois -h whois.nic.versicherung “nameserver 10.0.0.10”

Note: In the case where a host is registered for the origin of a delegated domain, i.e. both domain “example.versicherung” and nameserver “example.versicherung” exist, the query will match and return both the domain name and nameserver data objects.

1.4 WHOIS Output Format

The output format of the WHOIS server follows that outlined in Specification 4 of the “new gTLD agreement”:

Domain Name Data:

Domain ID: D1234567-TLD

Domain Name: EXAMPLE.TLD

Updated Date: 2009-05-29T20:13:00Z

Creation Date: 2000-10-08T00:45:00Z

Registry Expiry Date: 2010-10-08T00:44:59Z

Sponsoring Registrar: EXAMPLE REGISTRAR LLC

Sponsoring Registrar IANA ID: 5555555
Domain Status: clientDeleteProhibited
Domain Status: clientRenewProhibited
Domain Status: clientTransferProhibited
Domain Status: serverUpdateProhibited
Registrant ID: 5372808-GTLD
Registrant Name: EXAMPLE REGISTRANT
Registrant Organization: EXAMPLE ORGANIZATION
Registrant Street: 123 EXAMPLE STREET
Registrant City: ANYTOWN
Registrant State/Province: AP
Registrant Postal Code: A1A1A1
Registrant Country: EX
Registrant Phone: +1.5555551212
Registrant Phone Ext: 1234
Registrant Fax: +1.5555551213
Registrant Fax Ext: 4321
Registrant Email: EMAIL@EXAMPLE.TLD
Admin ID: 5372809-GTLD
Admin Name: EXAMPLE REGISTRANT ADMINISTRATIVE
Admin Organization: EXAMPLE REGISTRANT ORGANIZATION
Admin Street: 123 EXAMPLE STREET
Admin City: ANYTOWN
Admin State/Province: AP
Admin Postal Code: A1A1A1
Admin Country: EX
Admin Phone: +1.5555551212
Admin Phone Ext: 1234
Admin Fax: +1.5555551213
Admin Fax Ext:
Admin Email: EMAIL@EXAMPLE.TLD
Tech ID: 5372811-GTLD
Tech Name: EXAMPLE REGISTRAR TECHNICAL
Tech Organization: EXAMPLE REGISTRAR LLC
Tech Street: 123 EXAMPLE STREET
Tech City: ANYTOWN
Tech State/Province: AP
Tech Postal Code: A1A1A1
Tech Country: EX
Tech Phone: +1.1235551234
Tech Phone Ext: 1234

Tech Fax: +1.5555551213

Tech Fax Ext: 93

Tech Email: EMAIL@EXAMPLE.TLD

Name Server: NS01.EXAMPLEREGISTRAR.TLD

Name Server: NS02.EXAMPLEREGISTRAR.TLD

DNSSEC: Signed

DS Key Tag 1: 54135

Algorithm 1: 5

Digest Type 1: 1

Digest 1: <DIGEST>

DS Key Tag 2: 54135

Algorithm 2: 5

Digest Type 2: 2

Digest 2: <DIGEST>

% Copyright (c) 20XX by NIC.versicherung

% Restricted rights.

% Response generated on: 2011-10-13 11:11:25 UTC

Note that the “Domain Name” field will always contain the A-Label format of the domain. In cases where an IDN response is returned (and an appropriate character encoding was requested), the response will contain an additional field, the so-called “Domain U-Label”, containing the U-Label format of the respective Domain, for example:

Domain U-Label: exämple.versicherung

In the case where data for an unsigned domain is returned, the “DNSSEC” field will contain the value “unsigned” and the other DNSSEC-related fields will be excluded from the response.

Registrar Data:

Registrar Name: Example Registrar, Inc.

Street: 1234 Admiralty Way

City: Marina del Rey

State/Province: CA

Postal Code: 90292

Country: US

Phone Number: +1.3105551212

Fax Number: +1.3105551213

Email: registrar@example.tld

Registrar IANA ID: 55566677

% Copyright (c) 20XX by NIC.versicherung

% Restricted rights.

% Response generated on: 2011-10-13 11:11:25 UTC

Nameserver Data:

Server Name: NS1.EXAMPLE.TLD

IP Address: 192.0.2.123

IP Address: 2001:0DB8::1

Registrar: Example Registrar, Inc.

Registrar IANA ID: 55566677

% Copyright (c) 20XX by NIC.versicherung

% Restricted rights.

% Response generated on: 2011-10-13 11:11:25 UTC

1.5 Web-based RDDS

In addition to the command line based WHOIS service described above, the Registry Operator will, in line with requirements, provide a web-based WHOIS interface. The web-based interface supports the following classes of users in accordance with stated policies:

- The general public ("anonymous access"): Anonymous users can retrieve a limited amount of responses from the web based interface. To avoid unwanted bulk access and to prevent users from data harvesting the following access restrictions are deployed: (1) Client limits per day to be set based on source IPv4 and IPv6 addresses or blocks. (2) CAPTCHAs as a challenge-response test to ensure that the response is generated by a human being.
- Registrars and other authenticated users: Registrars and other approved users are issued with an authentication token that allows them to retrieve a greater number of WHOIS records via the web interface. Users qualifying in principal could for example include ICANN staff, URS or UDRP providers, and will be approved case by case by the registry.

All transactions on the web-based WHOIS are also logged and daily usage reports are sent to operations staff. The web-based WHOIS supports the same object types and query formats as the command line interface above, with the exception of the „-C" (character set) switch. The contents of a response from the web-based WHOIS service are also identical to the command line service, but may be reformatted and styled using HTML/CSS to aid presentation and display.

1.6 Searchable WHOIS

Searchable WHOIS functionality is not provided. This is to prevent bulk data harvesting and further data merging using extensive request combinations and Boolean search techniques. This is done intentionally to comply with data protection laws and privacy obligations.

Any request from legal institutions and law enforcement agencies for information outside of that supplied by any of the WHOIS services is dealt with directly by the legal department of the registry.

As a result there is no future intention to offer a broad search functionality, this applies to both the WHOIS protocol interface (port 43) and the web-based WHOIS interface

1.7 Lightweight RDDS Access ("Finger")

In addition to the required WHOIS interface a lightweight domain availability interface is supported. This interface is based on the "Finger" protocol, specified in RFC 1288, and exposes a very limited subset of data (already available in WHOIS), namely whether or not a certain domain name is available for registration. It provides faster response times than the standard WHOIS interface and places less load on the registry systems. The service will be operated accordingly:

- Lightweight access based on the "finger" protocol according to RFC 1288
- Lightweight access runs on finger.nic.versicherung on port 79
- No exposure of any information additional to that already available via the WHOIS RDDS
- Query format (command line example): "finger example.versicherung@finger.nic.versicherung"
- Response format (example): "example.versicherung IS NOT available"

1.8 IPv6 Support

All RDDS services (WHOIS, web-based WHOIS, Finger and bulk data access) fully support IPv6. In summary there is no difference in service quality levels or service responses between IPv4 and IPv6 for these services.

A detailed description of IPv6 support can be found in response to Question 36.

1.9 Service Level Compliance

The RDDS service complies with the SLA requirements (as defined in Specification 10) as follows:

Table Q26-01: please see attachment

1.1.1 RDDS Availability

The redundant and resilient architecture of the WHOIS system is described above, and is served by architecture as outlined in response to question 32. It is designed, at a minimum, to meet the required availability levels of 98%. It is understood that a reliable RDDS system is vitally important for TLD operations.

1.1.2 RDDS query RTT

The internal response time of the WHOIS system is significantly below the RDDS query RTT limit of 2000 ms so that it can be expected that for 95% of the queries this SLA requirement will be met. On test installations of the service, the query RTT is less than 500 ms, even in the event of a significant number of concurrent connections.

1.1.3 RDDS update time

Since the WHOIS system queries the “live” registry database, there is no update delay and hence the RDDS update time of 60 minutes for 95% of the updates can be assured.

2 Zone File Access

In accordance with Section 2 of Specification 4 of the Agreement („Zone File Access“), the Registry Operator will enter into an agreement with any internet user to provide access to download the zone file data and will cooperate as required with Centralized Zone Data Access (CZDA) Providers. This will be facilitated as follows:

- A dedicated FTP server will be set up for access to the zone file data. The name of that server will be: versicherung.zda.icann.org (pending allocation of that hostname by ICANN zone administrators). The zone file and associated checksum files will be available for download for the previous 3 days. Files will be generated once a day and named according to Section 2.1.3 of the Agreement.
- The file format follows exactly the specification which is based on the Master Zone File format defined in RFC 1035, according to Section 2.1.4 of the agreement.
- A specific user ID and password has to be assigned for each user to restrict access to accredited users and to prevent unauthorized access. This user has to access the server with this specific user ID to be able to transfer data.
- Access will be free of charge but limited to one download per day.
- All logins and data transfers are logged, monitored and reported. Access statistics will be available to the registry operator as well as to others if required.

The Registry Operator will also cooperate with ICANN and CZDA Providers as required in Section 2.2 of the agreement. Additional access is granted to ICANN itself (or its designee) and any designated Emergency Operator if required.

3 Bulk Registration Data Access

As an operator of a Thick Registry, the Registry Operator will operate in compliance with Section 3.2 of Specification 4 of the „new gTLD Agreement“ („Exceptional Access to Thick Registration Data“) as well as in compliance with Section 3.1 of Specification 4 („Periodic Access to Thin Registration Data“), and will provide ICANN with the required data in the required format.

The data will be provided in conformance with Specification 2 („Escrow“) of the Agreement, as required.

4 Resources

Regarding development of the RDDS interfaces, it shall be noted that most of the work is already complete at the time of this writing (eg. WHOIS and finger daemon are fully deployed and operational for other TLDs). Therefore, only minimal development work is required, and hence within TLD-Box's development team, only a half FTE is necessary (and planned for) for the continuous adaption and maintenance of the RDDS software itself.

For the actual operation of the RDDS interfaces, all technical operations staff members are trained on the various infrastructure and software components of the system, and manpower resources are accounted for in the general Network Operations Center budget.

The research & development team of the Registry Backend Operator is aware of ICANN's SSAC work regarding WHOIS (eg. http://www.icann.org/en/committees/security/sac051.pdf), and also participates in the IETF's proposed "WEIRDS" working group, in order to stay up-to-date with developments in the fields of domain data related publication services.

The RDDS makes use of virtual machines on the hardware provisioned for the TLD (and described in responses to Question 32 and 24). Therefore, no additional hardware resources are needed, however, the required bandwith in order to provide the RDDS services are accounted for in the general network topology of the Registry System.