GNSO gTLD Registry Constituency Statement

Issue: Inter-Registrar Transfer Policy Set A Request for Constituency Statements

Date: 2 October 2008

Issues Report URL: http://gnso.icann.org/issues/transfers/transfer-issues-report-set-a-23may08.pdf

General RyC Information

- Total # of eligible RyC Members[1]: 15
- Total # of RyC Members: 15
- Total # of Active RyC Members[2]: 15
- Minimum requirement for supermajority of Active Members: 10
- Minimum requirement for majority of Active Members: 8
- # of Members that participated in this process: 12
- Names of Members that participated in this process:

    1. Afilias (.info)
    2. DotAsia Organisation (.asia)
    3. DotCooperation (.coop)
    4. Employ Media (.jobs)
    5. Fundació puntCAT (.cat)
    6. mTLD Top Level Domain (.mobi)
    7. Museum Domain Management Association – MuseDoma (.museum)
    8. NeuStar (.biz)
    9. Public Interest Registry - PIR (.org)
    10. RegistryPro (.pro)
    11. The Travel Partnership Corporation – TTPC (.travel)
    12. VeriSign (.com & .net)

- Names & email addresses for points of contact
    - Chair: David Maher, dmaher@pir.org
    - Vice Chair: Jeff Neuman, Jeff.Neuman@Neustar.us
    - Secretariat: Cherie Stubbs, Cherstubbs@aol.com
    - RyC representative for this statement: Barbara Steele, bsteele@verisign.com

Regarding the issue noted above, the following positions represent the views of the ICANN GNSO gTLD Registry Constituency (RyC) as indicated. Unless stated otherwise, the RyC

[1] All top-level domain sponsors or registry operators that have agreements with ICANN to provide Registry Services in support of one or more gTLDs are eligible for membership upon the "effective date" set forth in the operator's or sponsor's agreement (Article III, Membership, ¶ 1). The RyC Articles of Operations can be found at http://www.gtldregistries.org/about_us/articles .

[2] Per the RyC Articles of Operations, Article III, Membership, ¶ 4: Members shall be classified as "Active" or "Inactive". A member shall be classified as "Active" unless it is classified as "Inactive" pursuant to the provisions of this paragraph. Members become Inactive by failing to participate in a Constituency meeting or voting process for a total of three consecutive meetings or voting processes or both, or by failing to participate in meetings or voting processes, or both, for six weeks, whichever is shorter. An Inactive member shall have all rights and duties of membership other than being counted as present or absent in the determination of a quorum. An Inactive member may resume Active status at any time by participating in a Constituency meeting or by voting.

positions were arrived at through a combination of RyC email list discussion and RyC meetings (including teleconference meetings).

1. **Issue 1 - Is there a way for registrars to make Registrant E-mail Address data available to one another? Currently there is no way of automating approval from the Registrant, as the Registrant Email Address is not a required field in the registrar Whois. This slows down and/or complicates the process for registrants, especially since the Registrant can overrule the Admin Contact**.

   1.1. If you believe policy change is needed, what options could be explored for registrars to make Registrant E-mail address data available? For each option, please identify how this would benefit automating approval, and, if any, what potential problems might be associated with this option.

      1.1.1. The members of the Registries Constituency recommend that Issue 1 be edited to clarify the scope of the issue.

      Specifically, it should be noted that registry WHOIS is authoritative which would include, in the case of thick registries, the registrant contact information such as e-mail address. Also, in the case of thick registries, the registry agreements mandate that the registry operator display the registrant e-mail address in the registry's WHOIS.

      At least one thick registry which is subject to privacy laws has implemented a tiered access approach to publishing WHOIS information.

      Any changes to the policy and/or practice should be limited to addressing the issue of obtaining authoritative information relating to the administrative contact e-mail address in those instances where it is not available via the registry WHOIS. In the case of thin registries, the contact information for a domain name in the registrar WHOIS (including the registrant e-mail address) is authoritative. In this case, registrars could implement a tiered access approach to providing WHOIS information that would permit the private provision of Registrant e-mail address and thereby satisfying various privacy law requirements.

   1.2. Please identify examples or best practices of email address use to facilitate and/or automate approval from a Registrant for a transfer.

      1.2.1. The members of the Registries Constituency agree that authentication of the identity of the registrant, as stipulated by the IRTP, is the responsibility of the Gaining Registrar. Therefore, aside from EPP AuthInfo authentication which is systematically enforced when an EPP Registry processes a transfer command, Registrars are best able to address this item.

   1.3. Although it is not the purpose of this Policy Development Process (PDP) to recommend changes to WHOIS policy, it conceivably could be an option to require registrant email addresses in WHOIS. The Working Group is interested in your views on that potential option, without regard to the broader WHOIS issues of availability and accuracy of WHOIS data. The Working Group is more particularly interested in your views about any other options not involving WHOIS.

      1.3.1. As previously indicated, thick registries are already publishing registrant e-mail addresses in WHOIS. For thin registries to add contact information would be a major change resulting in significant cost and time to deploy. Registrars are already dealing with this requirement and thus extending this requirement to their local WHOIS operations for use with thin registries does not seem to extend a further burden on registrars and their handling of privacy issues than already exists.

   1.4. **Level of Support of Active Members**: Supermajority

1.4.1. # of Members in Favor: 12

1.4.2. # of Members Opposed: 0

1.4.3. # of Members that Abstained: 0

1.4.4. # of Members that did not vote: 3

1.5. **Minority Position**: None

1.6. **General impact on the RyC**: Minimal

1.7. **Financial impact on the RyC**: Minimal

1.8. **Analysis of the period of time that would likely be necessary to implement the policy**: Not applicable as those registries that currently have registrant contact information are already publishing the e-mail address. For thin registries to add contact information would be a major change resulting in significant cost and time to deploy.

2. Issue 2 - Whether there is need for other options for electronic authentication (e.g., security token in the Form of Authorization (FOA)) due to security concerns on use of email addresses (potential for hacking or spoofing).

2.1. What security concerns can you identify related to current ways of authenticating registrants. Note, the Security and Stability Advisory Committee (SSAC) has identified a risk of email spoofing for purposes of domain name hijacking, see link. We are interested in your views on this and any other concerns.

2.1.1. The members of the Registries Constituency recognize that use of the e-mail address has certain weaknesses, but the merits and costs of implementing other methods should be judged in their own right and not against any inadequacies and inefficiencies of email.

2.2. Do you think there is a need for other options for electronic authentication? Please state the reasons for your answer.

2.2.1. The members of the Registries Constituency support allowing market forces to operate freely in this area. Registrars can measure demand to determine if they want to implement additional security methods for authenticating transfer requests. Registrars should be permitted to differentiate themselves from their competitors by determining what offerings they make available to registrants, including the level of security they employ in protecting the contact information of the Registrants of domain names.

2.3. Do you know of any Registrars using additional means for electronic authorization (e.g. security token, digital signatures, etc.)? If so, what are they and who offers them?

2.3.1. The Registries Constituency believes that some registrars have implemented additional security methods to authenticate transfers of domain names. Specifically, Markmonitor, GoDaddy and Moniker have products available to provide additional security. More information relating to these products can be found at the following websites, respectively: http://www.markmonitor.com/products/domain_management.php, https://www.godaddy.com/gdshop/protect/landing.asp?isc_prg001&ci=9004 and http://www.domainmaxlock.com/. We also have confirmation that CSC will issue some customers Secure ID tokens (RSA) for additional validation.

2.4. If a need would be identified for other options of electronic authentication, what other options could be explored?

2.4.1. The EPP AuthInfo code provides an automated mechanism to authenticate transfer requests and could take the place of both the Registrant and Admin Contact e-mail addresses.

2.5. Of those other options to be explored, please identify the potential benefits but also any potential problems.

2.5.1. Use of the AuthInfo code to authenticate transfers is already in place and required by all EPP registries or the transfer command will fail. There is no

additional cost or development required to implement this method of authentication. The IRTP addresses the potential problems associated with obtaining the AuthInfo code for a domain name in Section 5.

However, for the use of AuthInfo codes to be effective, the members of the Registries Constituency agree that compliance with the requirement that AuthInfo codes be unique by domain name must be enforced via the ICANN Registrar Compliance Program. Enforcement of unique AuthInfo codes by domain name should not be done by the registry operator as such enforcement would create a negative response for conflicting AuthInfo codes thus creating a mechanism to test for in-use AuthInfo codes which could result in a security exposure.

While the use of security tokens by the Registrant to authenticate a transfer would bring additional security to the transfer process, the members of the Registries Constituency agree that market forces should be allowed to work freely in this regard and demand should dictate whether a Registrar elects to employ this method since the expense and logistics of providing tokens to all Registrants may not make this a feasible option for all registrars and registrants.

2.6. Do you have or know of any data in relation to the impact of the Extensible Provisioning Protocol (EPP) deployment on security in relation to authentication? If so, please describe the source and type of data.

2.6.1. No members of the Registries Constituency are aware of any security issues relating to the deployment of EPP or AuthInfo codes. All indications are that the RFC is stable and EPP and AuthInfo codes, when properly implemented, are secure.

It should be noted that EPP requires mutual authentication of clients/registrars and servers before a Transport Layer Security (or TLS) connection can be made between the two parties. Digital certificates, digital signatures, and PKI services are used to authenticate both parties. Certificates must be signed by a CA that is recognized by the server operator. [RFC 4934, section 8]

Additionally, all EPP clients/registrars are required to identify and authenticate themselves using a server-assigned user ID and a shared secret (a password) that is sent to the server using a login command. The server must confirm the identity and shared secret before the client is given access to other protocol services. [RFC 4930, section 2.9.1.1]

Some EPP commands, such as the domain transfer command, require additional authentication information that must be provided and confirmed before the requested action is completed. The default authentication information service uses a shared secret (or AuthInfo code) that is known to the registry, the registrar, and the registrant. Registrants are required to provide this secret to a second registrar when requesting the second registrar to initiate a domain transfer on the registrant's behalf. The authentication information data structure is extensible so that additional authentication mechanisms can be defined and implemented in the future. [RFC 4931, sections 3.2.1 and 3.2.4]

2.7. Do you know of any further examples, apart from those mentioned in the issues report (.uk registry and .se registry), of electronic authentication methods? If so, what are they and who offers them?

2.7.1. The members of the Registries Constituency are unaware of any methods of electronic authentication currently in use other than those indicated in section 2.3.1 of this Issue #2.

2.8. **Level of Support of Active Members**: Supermajority

2.8.1. # of Members in Favor: 12

2.8.2. # of Members Opposed: 0

2.8.3. # of Members that Abstained: 0

2.8.4. # of Members that did not vote: 3

2.9. **Minority Position**: None

2.10. **General impact on the RyC**: To be determined.

2.11. **Financial impact on the RyC**: To be determined.

2.12. **Analysis of the period of time that would likely be necessary to implement the policy**: The period of time to implement other security methods could range from no time required to many months depending on which methods implemented. More information is needed to determine this.

3. Issue 3 - Whether the policy should incorporate provisions for handling "partial bulk transfers" between registrars – that is, transfers involving a number of names but not the entire group of names held by the losing registrar.

3.1. Should the policy incorporate provisions for handling "partial bulk transfers" between registrars? Please state the reasons and use-cases for your answer.

3.1.1. The members of the Registries Constituency support the incorporation of provisions for handling partial bulk transfers between registrars provided that the provisions would not require reengineering of the existing bulk transfer functionality or new development. Specifically, the transfer of the specified domain names would not extend the term of the registration by an additional year and the registration fee would not be assessed. Specific details of the product offerings by registries and registrars should be left up to the individual registries and registrars and should be driven by market demand.

3.2. Are you aware of any voluntary provisions to facilitate partial bulk transfers? If so, could you please provide further details on those provisions (apart from those already identified in the issues paper – NeuLevel (.biz), Nominet (.uk)).

3.2.1. The only voluntary provisions to facilitate partial bulk transfers that the members of the Registries Constituency are aware of are those that have been identified (i.e., NeuStar and Nominet).

3.3. **Level of Support of Active Members**: Supermajority

3.3.1. # of Members in Favor: 12

3.3.2. # of Members Opposed: 0

3.3.3. # of Members that Abstained: 0

3.3.4. # of Members that did not vote: 3

3.4. **Minority Position**: None

3.5. **General impact on the RyC**: Minimal

3.6. **Financial impact on the RyC**: Minimal

3.7. **Analysis of the period of time that would likely be necessary to implement the policy**: If current technology is used, there would be no system / software development time required at the registries. However, implementation time to develop requirements / products involving submission by the registrar of partial bulk transfer requests could take 3 to 12 months.