Draft Final Report on the

Inter-Registrar Transfers Policy - Part A

Policy Development Process

STATUS OF THIS DOCUMENT

This is the Final Report on IRTP Part A PDP, prepared by ICANN staff for submission to the GNSO Council on XXX following following public comments on the Initial Report of 9 January 2009.

SUMMARY

This report is submitted to the GNSO Council following public comments to the Initial Report as a required step on GNSO Policy Development Process on Inter-Registrar Transfers Policy.

TABLE OF CONTENTS

1. Executive Summary

1.1 Background

- The Inter-Registrar Transfer Policy (IRTP) aims to provide a straightforward procedure for domain name holders to transfer their names from one ICANN-accredited registrar to another should they wish to do so. The policy also provides standardized requirements for registrar handling of such transfer requests from domain name holders. The policy is an existing community consensus policy that was implemented in late 2004 and is now being reviewed by the GNSO.
- The IRTP Part A Policy Development Process (PDP) is the first in a series of five PDPs that address areas for improvements in the existing transfer policy.
- The IRTP Part A PDP concerns three "new" issues: (1) the potential exchange of registrant email information between registrars, (2) the potential for including new forms of electronic authentication to verify transfer requests and avoid "spoofing," and (3) to consider whether the IRTP should include provisions for "partial bulk transfers" between registrars.
- A Working Group was formed on 5 August 2008.

1.2 Deliberations of the Working Group

- The Working Group worked on the three different issues in parallel to the preparation of constituency statements and the public comment period on this topic.
- In relation to Issue I - 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 – the Working Group discussed the following topics; the Extensible Provisioning Protocol (EPP), Internet Registry Information Service (IRIS), Registrant vs. Admin contact approval, Thin vs. Thick registries, Whois and the AuthInfo code.

- In relation to Issue II – 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) – the Working Group discussed the incidence of hijacking and the possibility of additional security measures.
- In relation to Issue III – 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 – the Working Group discussed whether partial bulk transfers concern transfers between registrars or also include transfers between registrants and registrars, what would constitute a partial bulk transfer and how the existing policy for a bulk transfer could potentially be used for a partial bulk transfer,

1.3 Preliminary Conclusions of the Working Group

- For all issues, it should be noted that the Working Group will not make a final decision on which solution(s), if any, to recommend to the GNSO Council before a thorough review of the comments received during the public comment period and final constituency statements has taken place.
- Issue I - Is there a way for registrars to make Registrant E-mail Address data available to one another?
  The WG noted that WHOIS was not designed to support many of the ways in which it is currently used to facilitate transfers. Some members suggested that finding a way to make the Registrant e-mail address more readily available could be addressed as part of an overall technical modernization of the WHOIS protocol. This could be through updates to the existing protocol, modification of the Extensible Provisioning Protocol (EPP) or adoption of the Internet Registry Information Service (IRIS) protocol. However, after review and discussion none of these options received broad agreement.

  The WG did note that, in the absence of a simple and secure solution for providing gaining registrar access to the registrant email address, future IRTP working groups should consider the appropriateness of a policy change that would prevent a

registrant from reversing a transfer after it has been completed and authorized by the admin contact. This option would not change the current situation whereby a losing registrar can choose to notify the registrant and provide an opportunity to cancel a transfer before the process is completed.

- Issue II - Whether there is need for other options for electronic authentication?
  Based on the discussion in the Working Group, there appears to be broad agreement that there is a need for other options for electronic authentication. However, opinions in the Working Group differ as to whether these options should be developed by means of GNSO policymaking or should be left to market solutions.

- Issue III - Whether the policy should incorporate provisions for handling partial bulk transfers between registrars?
  Based on the discussion in the Working Group, there appears to be broad agreement that there is no need to incorporate provisions for handling partial bulk transfers between registrars at this stage. The Working Group believes that these scenarios can be addressed either through the existing Bulk Transfer provisions, or through existing market solutions.

1.4 Initial Constituency Statements & Initial Public Comment Period

- The public comment period ran from 5 September 2008 to 29 September 2008. Apart from the Constituency statements, two other comments were received. However, these two comments were deemed off-topic.
- Constituencies were requested to use the Constituency Statement Template the Working Group developed to provide their feedback. Input was received from the Intellectual Property Interests Constituency, gTLD Registry Constituency, Registrars Constituency and the Business and Commercial Users' Constituency. Constituency statements received are reflected per issue in chapter 6 of this report, and are set forth in their entirety in Annex B.
- It should be noted that the views of the Constituencies may differ from the views expressed by the Working Group. The Constituency statements should therefore be reviewed in their entirety.

1.5 Conclusions and Next Steps

- The Working Group aims to complete this section of the report in the second phase of the PDP, following a second public comment period and the submission of the final constituency statements.

2.   Objective and Next Steps

This Final Report on the Inter-Registrar Transfer Policy Part A PDP is prepared as required by the GNSO Policy Development Process as stated in the ICANN Bylaws, Annex A (see http://www.icann.org/general/bylaws.htm#AnnexA). It is based on the Initial Report of 9 January 2009 and reflects the comments received on both documents. This report is submitted to the GNSO Council for the Council's consideration. The conclusions and recommendations for next steps on the three issues included in this PDP are outlined in Chapter 7.

3.   Background

3.1   Process background

- Consistent with ICANN's obligation to promote and encourage robust competition in the domain name space, the Inter-Registrar Transfer Policy (IRTP) aims to provide a straightforward procedure for domain name holders to transfer their names from one ICANN-accredited registrar to another should they wish to do so. The policy also provides standardized requirements for registrar handling of such transfer requests from domain name holders. The policy is an existing community consensus policy that was implemented in late 2004 and is now being reviewed by the GNSO.

- As part of that review, the GNSO Council formed a Transfers Working Group (TWG) to examine and recommend possible areas for improvements in the existing transfer policy. The TWG identified a broad list of over 20 potential areas for clarification and improvement (see http://www.icann.org/en/gnso/transfers-tf/report-12feb03.htm).

- The Council tasked a short term planning group to evaluate and prioritize the policy issues identified by the Transfers Working Group. In March 2008, the group delivered a report to the Council that suggested combining the consideration of related issues into five new PDPs (see http://gnso.icann.org/drafts/transfer-wg-recommendations-pdp-groupings-19mar08.pdf).

- On 8 May 2008, the Council adopted the structuring of five additional inter-registrar transfers PDPs as suggested by the planning group (in addition to a recently concluded Transfer PDP 1 on four reasons for denying a transfer). It was decided that the five new PDPs would be addressed in a largely consecutive manner, with the possibility of overlap as resources would permit.

- The Council requested an Issues Report from Staff on the first of the new PDP issue sets (Set A – New IRTP Issues) that was delivered to the Council on 23 May 2008 (see http://gnso.icann.org/issues/transfers/transfer-issues-report-set-a-23may08.pdf).

- The three "new" issues in Set A address (1) the potential exchange of registrant email information between registrars, (2) the potential for including new forms of

electronic authentication to verify transfer requests and avoid "spoofing," and (3) to consider whether the IRTP should include provisions for "partial bulk transfers" between registrars.

- The GNSO Council resolved on 25 June 2008 to launch a PDP ("PDP June-08") on these three issues and adopted a charter for a Working Group on 17 July 2008.

3.2   Issue Background (excerpt from Issues Report)

- Please note that the following text has been excerpted from the issues report and does not contain any new input from the Working Group.

   Issue I – Potential exchange of registrant e-mail information

- Issue I – "Whether there could be a way for registrars to make Registrant Email 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."

- Section 1.1 of the Transfer Policy identifies the Registrant and the Administrative Contact as parties who can authorize a transfer, and notes that the Registrant's authority supersedes that of the Administrative Contact. Accordingly, an authorization from the Registrant provides a reliable ground for executing a transfer, while an authorization from the Administrative Contact can be contested by the Registrant, in spite of being recognized as a valid ground for a transfer. A convenient means to acquire Registrant authorization could thus enable a reduction of the number of contested transfers.

- During its deliberations, the Transfers Working Group noted that the issue is related to the Whois provisions, since the email address of the Administrative Contact is a required field in Whois, in contrast to the Registrant email address. However, in the context of a PDP focused on the Transfer Policy, any proposed policy change affecting Whois policy (for example requiring registrant email information in the Whois) would be outside the scope of the PDP[1]. The issue to address is thus limited

---

[1] Based on the discussions of the Working Group it should be noted that these two sentences draw a conclusion that has not been made by the GNSO Council or the Working Group, but are carried over from an earlier Staff Issues Report. See Section 5 regarding Whois below.

---

to other means of keeping, maintaining and exchanging registrant email information between the relevant Registrars. This invokes procedural, administrative and security aspects."

Issue II – Options for Electronic Authentication

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

- The original Transfers Task Force mentioned this issue as follows in its Final Report:
   19. In the event that the Gaining Registrar must rely on a physical process to obtain this authorization, a paper copy of the Standardized Form of Authorization will suffice insofar as it has been signed by the Registrant or Administrative Contact and is accompanied by a physical copy of the Losing Registrar's Whois output for the domain name in question.
   a – b […references to physical documents, of no relevance here.]
   c. The Task Force notes support for the concept that in the event of an electronic authorization process, recommended forms of identity would include;
   • electronic signature in conformance with national legislation, for instance, the United States e-Sign Act
   • Email address matching Registrant or Administrative Contact email address found in authoritative Whois database.
   In relation to the first bullet point above, it can be noted that the current extent of Registrars' use of digital signature means for transfers is unknown. Such information could be useful to collect as background for deliberations in a future PDP covering this issue.

- The Transfers WG noted the issue in its report as follows:
   According to the policy, the Gaining Registrar is required to obtain the FOA from the Registrant or Administrative Contact before initiating a transfer request. The Registrar of Record also has the option to send an FOA to confirm the transfer request. Policy issues relating to the FOA include:

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

- Regarding the risk of spoofing mentioned by the Transfers WG, useful background information is provided in the SSAC report on domain name hijacking, available at http://www.icann.org/announcements/hijacking-report-12jul05.pdf. Recommendation 10 of this report states: "ICANN should consider whether to strengthen the identity verification requirements in electronic correspondence to be commensurate with the verification used when the correspondence is by mail or in person."

- The SSAC report was produced in 2005 and it should be noted that, since then, Extensible Provisioning Protocol (EPP) has been deployed by all gTLD registries that have implemented the Transfer Policy. Since EPP requires an authorization ("AuthInfo") code, EPP deployment may have had an impact from a security standpoint and recent data in this respect could be useful as background for a future PDP covering this issue.

- It can also be noted that some ccTLDs do use electronic authentication methods for transfers, for example through digital signatures for authentication of e-mail requests. The .UK registry operator Nominet uses PGP as described at http://www.nic.uk/registrars/systems/auto/pgp/. Another example is the .SE registry operator, IIS, featuring a certificate-based web interface ("Domänhanteraren" – in English "The Domain Handler") for the registrant, where the registrant can effectuate changes of domain information, including change of Registrar, see https://domanhanteraren.iis.se/start/welcome. There may be other such examples of interest as references for this issue."

Issue III - Provisions for partial bulk transfers between Registrars

- Issue III – "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.

- This aspect was not touched upon by the Transfers Task Force, but identified as a potential issue (under "Other") by the Transfers WG in its report.

- Part B of the Transfer Policy governs bulk transfers, meaning transfer of all domains sponsored by one Registrar to another Registrar, for example as a consequence of one Registrar acquiring another. According to the policy, bulk transfers can only take place under certain specific conditions, for further information see part B at http://www.icann.org/transfers/policy-12jul04.htm.

- While different from bulk transfers in the "complete" sense, i.e. transfer of a Registrar's complete domain portfolio to another Registrar, the need for "partial" bulk transfers can arise due to, for example, company takeovers, where the acquiring company wishes to transfer some or all of the acquired company's domains to its own Registrar of Record. There is no prescribed way of doing so in the Inter Registrar Transfer Policy other than domain by domain, although Registrars are free to accept, for example, fax lists with numerous domains to transfer, while still having to follow the authentication/verification practices of the policy. The extent of such "voluntary provisions to facilitate partial bulk transfers" in practice is unknown.

- NeuLevel,Inc., the registry operator of .BIZ, has proposed the launch of a partial bulk transfer service, which has been approved by ICANN through the Registry Services Technical Evaluation Panel (RSTEP) procedure. This service proposal was prompted by two Registrars' request for a partial bulk transfer between them. For further information, see http://www.icann.org/registries/rsep/NeuLevel_request.pdf.

- For information, there are provisions in place for partial bulk transfers in some ccTLDs. The .UK registry, Nominet, has a procedure for "mass transfers", described at http://www.nic.uk/registrants/maintain/transfer/mass/ and also for PGP-signed "bulk" operations at the registrar level, described at http://www.nic.uk/registrars/systems/auto/bulk/ (see especially Example 9 therein, of relevance for partial bulk transfers). There may be other such examples of interest as references for this issue."

4.   Approach taken by the Working Group

The IRTP Part A Working Group started its deliberations on 5 August 2008 where it was decided to continue the work primarily through weekly conference calls and e-mail exchanges. The Working Group agreed to start working on the three different issues in parallel to the preparation of constituency statements and the public comment period on this topic. In order to facilitate the work of the constituencies, a template was developed for responses (see Annex A).

4.1   Members of the IRTP Part A Working Group

The members of the Working group are:

Name	Constituency / other	Affiliation
Paul Diaz (Chair of the Working Group)	Registrar	Network Solutions
James M. Bladel	Registrar	Go Daddy
Mike Rodenbaugh (Council liaison)	Business	Rodenbaugh Law
Barbara Steele	Registry	Verisign
Kevin R. Erdman	IPC	Baker & Daniels LLP
Sebastien Bachollet	ALAC	ISOC France
Mike O'Connor	Business	O'Connor Company
Marc Trachtenberg	IPC	Winston & Strawn LLP
Margie Milam	Registrar	Markmonitor
Mark Klein	Registrar	Sedo
Michael Collins	Business	Internet Commerce

		Association
Steven Vine	Registrar	Register.com
Adam Eisner	Registrar	Tucows
Avri Doria (GNSO Chair)	NCUC	Luleå Univ of Tech
Chuck Gomes (GNSO Vice Chair)	Registry	Verisign

The statements of interest of the Working Group members can be found at http://gnso.icann.org/issues/transfers/soi-irtp-a-pdp-oct08.shtml.

The email archives can be found at http://forum.icann.org/lists/gnso-irtp-pdp-jun08/.

5. Deliberations of the Working Group

This chapter provides an overview of the deliberations of the Working Group conducted both by conference call as well as e-mail threads. The points below are just considerations to be seen as background information and do not necessarily constitute any suggestions or recommendations by the Working Group.

Issue I - 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.

Extensible Provisioning Protocol (EPP)

▪ One idea discussed in the context of issue I was to extend or modify the Poll Message facility of the Extensible Provisioning Protocol (EPP) for this function (see Annex C for further details on EPP). EPP is currently used as an authenticated and secure channel of communication between the Registry and Registrar, which can also be used in the context of transfers (see figure 1).

▪ The Poll Message system has the advantage of being both an authenticated and secure channel of communication between the Registry and Registrar, but it is currently mostly unidirectional (Registrar does not create messages for Registry) and there is no means for registrars to communicate with each other. The Working Group considered whether EPP could be extended to allow registrars to create Poll Messages for each other, for those situations which require the sharing of registrant information. Issues such as security, costs of implementation and feasibility would need to be addressed in order to determine whether this is a suitable option, but overall the Working Group considers this a possible avenue to be further explored.

Figure 1.

Transfer in an EPP Registry
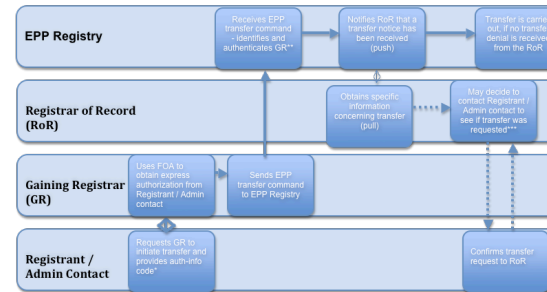
Notes

* Registrars must provide the Registered Name Holder with the unique "AuthInfo" code within five (5) calendar days of the Registered Name Holder's initial request if the Registrar does not provide facilities for the Registered Name Holder to generate and manage their own unique "AuthInfo" code.

** EPP requires mutual authentication of clients/registrars and servers before a 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 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].

*** The Registrar of Record has 5 calendar days to respond to transfer notice from Registry

- It should be noted that the RFC3730 - Extensible Provisioning Protocol (EPP) did not foresee the potential use of poll messages in this way which may mean that a modification of the RFC would be required in order to consider this as an option. Such a modification could take a substantial amount of time. In addition, the implementation of a modified EPP would bring with it certain costs. Both elements would need to be considered prior to making a recommendation.
- In relation to the security of EPP, it was noted that no security incidences with EPP have been reported to date (or at least not to the knowledge of the Working Group members).

Internet Registry Information Service (IRIS)

- The Internet Registry Information Service (IRIS) has been developed by the IETF Cross Registry Internet Service Protocol (CRISP) working group with the objective to replace Whois. IRIS offers the opportunity to set some enforceable standards around who has access to specific registrant data fields and a way to control such access.
- Not taking into account or providing any opinion on whether IRIS should or should not be considered as a replacement for Whois, the Working Group discussed whether it would be an option to consider IRIS as a secure means of communication between registrars. In this circumstance, the only data that would be provided and shared between registrars would be registrant e-mail data. The Authinfo code could be used as a means of authentication to access IRIS.
- As with EPP, the costs and time of implementation would need to be assessed in order to determine whether this would be a viable option.
- IRIS was also raised as a possible solution for the secure transmission of data between registrars and/or registries in one of the comments submitted during the public comment period on the Initial Report (see section 6.4 for more details).

Registrant vs. Admin contact approval

- While a registrant has the ultimate authority regarding an inter-registrar transfer, the admin contact can initiate and approve a transfer without a registrant's involvement. Most registrars, maybe all, will notify the registrant that a transfer has been initiated and that the registrant can cancel it and that the transfer will go through if the registrant does

nothing. So, if a registrant finds that the admin contact has transferred a domain away without registrant approval this can lead to a transfer dispute.

- Any policy that allows one person to authorize a transfer and another person to dispute the transfer after it is completed is a potential source of conflict.
- Taking this into account, one could consider requiring registrant approval before a transfer occurs which would normally avoid most disputes.
- Another option would be to give the admin contact the ultimate transfer authority. However, this might result in additional security / hijacking risks as the admin contact details are part of the public Whois.
- Similarly, the registrant could be given the sole transfer authority. However, this brings us back to the issue at hand, how to make the registrant e-mail address available to the gaining registrar in order to confirm a transfer request.
- Those registrars participating in the Working Group confirmed that normally the Gaining Registrar sends the confirmation of a transfer to the admin contact since that is the contact that they have on file. It could be considered to make it a requirement, instead of optional, that the Registrar of Record confirms the transfer with the Registrant (instead of the admin contact). This would add another approval into the process that could enable a losing registrar to delay or prevent a transfer. When combined with other transfer process items that a losing registrar controls and can use to cause difficulties and delay, registrar lock removal and auth code retrieval, adding a requirement for the loosing registrar to confirm the transfer has the potential of causing insurmountable difficulty and delay for registrants especially when trying to transfer a large domain name portfolio. However it would resolve the problem of Registrant e-mail not being publically available and it would resolve the problem of domain transfers being authorized by the admin contact without the Registrant's consent.

Thin vs. Thick Registries

- A "Thin" Registry is one for which the Registry database contains only domain name service (DNS) information:
  - Domain name
  - Name server names
  - Name server address

- The name of the Registrar
- Basic transaction data

- It does not contain any Registrant or contact information. Registrant or contact information is maintained by the Registrar. Examples of Thin registries are .com, .net and .jobs (see table 1 for a complete overview).
- A "Thick" Registry is one for which the Registry database contains:
  - Registrant and contact information
  - Domain name
  - Name server names
  - Name server address
  - The name of the Registrar
  - Basic transaction data
- All authoritative information is kept within the Registry.
- Registrant Email is collected and maintained by all registrars, and submitted to all "Thick" Registries. A check of gTLD WHOIS data shows that Registrant Email is also displayed for all Thick Registries.
- "Thin" registries do not maintain any registrant information.
- It should be noted that "Thick" registries are not obliged to include the registrant e-mail address in Whois data, so requiring all "Thin" registries to become "Thick" registries would not change anything for the particular issue at hand, unless the inclusion of the registrant e-mail address would be mandated.
- If the registrant email address would be required for inclusion in Whois data, it should not even matter whether it is the registry or the registrar that is required to maintain Whois data.

Table 1

gTLD	Thin	Thick
.ARPA		✓
.AERO		✓
.ASIA		✓
.BIZ		✓

	Thin	Thick
.CAT		✓
.COM	✓	
.COOP		✓
.EDU		✓
.GOV		✓[2]
.INFO		✓
.INT		✓
.JOBS	✓	
.MIL		✓[3]
.MOBI		✓
.MUSEUM		✓
.NAME	✓	✓[4]
.NET	✓	
.ORG		✓
.PRO		✓
.TEL		✓
.TRAVEL		✓

Whois

- The WG agreed that even though Whois should not be the main topic of the discussion as it is not specifically in the remit of this Working Group to make any recommendations for Whois modification, it would not be off-limit to include in the discussion if deemed appropriate for providing an insight into issue I.
- Registrant email addresses are not a required WHOIS field. Registrars can publish it if they choose. Requiring that this address be made publicly available would solve the issue at hand, but at the same time it might raise privacy and security concerns - and is possibly beyond the mandate of this WG.

---

[2] Presumed thick Whois – Whois data not publicly available
[3] Presumed thick Whois – Whois data not publicly available
[4] 'Thick' Whois information is available, but only after payment

- Members of the RyC who provided feedback also indicated that ICANN Registry Agreements require that the registrant e-mail address field be displayed in the WHOIS of most gTLDs and sTLDs and most of those registries make submission and display of registrant e-mail address mandatory. It should be noted that this only applies to 'thick' registries.

AuthInfo Code
- The Working Group also discussed whether the AuthInfo code, which is currently being used to authenticate a transfer in EPP based registries, could be used as a means to authenticate the transfer instead of the registrant or admin contact e-mail address.
- It was noted that this would not solve the issue at hand as the registrant could still challenge a transfer, even if the AuthInfo code would be provided by the admin contact, unless the submission of a valid AuthInfo code would be the only requirement to initiate a transfer. However, this was not deemed a secure and viable solution compared to the current system.
- One suggestion made during the public comment period on the Initial Report was to consider using the AuthInfo code to retrieve information from the domain:info or contact:info operation in the EPP protocol, although this would only work for thick registries (see section 6.4 for more details).

Conclusion for Issue I

- The WG noted that WHOIS was not designed to support many of the ways in which it is currently used to facilitate transfers. Some members suggested that finding a way to make the Registrant e-mail address more readily available could be addressed as part of an overall technical modernization of the WHOIS protocol. This could be through updates to the existing protocol, modification of the Extensible Provisioning Protocol (EPP) or adoption of the Internet Registry Information Service (IRIS) protocol. However, after review and discussion none of these options received broad agreement.

The WG did note that, in the absence of a simple and secure solution for providing the gaining registrar access to the registrant email address, future IRTP working groups should consider the appropriateness of a policy change that would prevent a registrant

---

from reversing a transfer after it has been completed and authorized by the admin contact. This option would not change the current situation whereby a losing registrar can choose to notify the registrant and provide an opportunity to cancel a transfer before the process is completed.

Issue II - 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).

- The Working Group also noted that the loss of even a single domain name through "hijacking" can be personally and financially disruptive to a registrant and could result in significant exposure to liability for the involved registrar.
- One member of the Group shared information on the incidence of hacking and spoofing and that the respective company has the equivalent of 1-2 full-time employees dedicated to work on this specific issue. Since January 2008, this team has received over 1000 claims of domain name "hijacking," and has taken action to restore the original registrant in 533 of these cases, and upheld the transfer in another 504. On average, the investigation of each claim takes 5-10 business days. Some of these incidents are internal (e.g. Change of Registrant) transfers, not transfers from other registrars. It should be noted that AuthInfo keys are only involved in the latter case. The "vast majority" of disputed transfers involved compromised email accounts. Typically, these are free accounts (Gmail, Yahoo, Hotmail, etc.). These figures demonstrate that the prevention and remediation of domain name "hijacking" is a significant operational burden for registrars.
- Additional security measures could be considered, but it should be noted that this would result in additional costs. Furthermore, it is argued that any recommendation to this end should not result in mandating certain technologies over others.
- Some members of the Working Group considered that offering additional security measures should be left as a service that a registrar can choose to provide as part of its offering.

Conclusion for Issue II

- Based on the discussion in the Working Group, having taking into account the comments received during the public comment periods and constituency statements, there appears to be broad agreement that there is a need for other options for electronic authentication. However, opinions in the Working Group differ as to whether these options should be developed by means of GNSO policymaking or should be left to market solutions.

Issue III - 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.

- Some members of the Working Group argue that this issue relates to potential partial bulk transfers between registrars, and not registrant initiated partial bulk transfers which are in practice already possible and offered as a service by a number of registrars.
- Several members of the Working Group noted that if there would be support for incorporating provisions for handling partial bulk transfers, it is imperative to ensure that these provisions do not blur the boundaries between Policy requirements and Product development.
- In order to consider this issue in its full depth, it will be important to define what would constitute a partial bulk transfer. What would be a minimum, would these transfers be treated as renewals, is there a fee involved? Also, this definition process would need to take into consideration that partial bulk transfers should not be abused by those trying to avoid the charge that currently applies for bulk transfers over 50,000 domain names.
- There is a policy in place that defines how a bulk transfer process works (see ICANN Policy on Transfer of Registrations between Registrars, 12 July 2004, Section B. ICANN-Approved Transfers). When a registry executes a bulk transfer under the existing policy, the registries receive approval from ICANN to use the 'bulk transfer tool' to transfer all domains under the management of one ICANN accredited registrar to another designated ICANN accredited registrar. The registry then contacts both the gaining registrar and the losing registrar to coordinate a time to complete the transfer. A script is run that, in essence, only changes the registrar of record for the domain names - the expiration date is not changed nor is a registration fee assessed.

- It was suggested that a similar process could be considered for a 'voluntary partial bulk transfer' request with the exception that the request would not be received from ICANN, but instead, from one of the registrars. Therefore, the registries would receive the request to initiate a voluntary partial bulk transfer from a registrar and, provided all requirements are met, the registry would execute the command to move the designated domain names from the losing registrar to the gaining registrar (without further intervention by the registrars and without moving the expiration dates of the domain names forward or assessing the standard registration fee to the gaining registrar). The details surrounding the minimum requirements for submission of requests would need to be addressed. Much work would need to be done by the WG to define the requirements, fee structure, etc. The requirements should be limited to those relating to registry and registrar responsibilities. How various registrars decide to develop products (and establish their fee structure that they would charge for the service to their registrants), as well as market the product to their registrants, should be left up to the individual registrars.
- It was noted that from a security perspective, provisions for a partial bulk transfer might not be desirable as this would also allow miscreants to transfer a large number of domain names at once.
- Having taken into account the above considerations, the Working Group started deliberations on the possible scenarios in which a partial bulk transfer might be appropriate and found the following:
  - o Scenario I – Partial Bulk Transfer following ICANN accreditation of a reseller
    A reseller becomes an ICANN accredited registrar and may decide to become the registrar or record for those domain names for which it has been accredited.
  - o Scenario II – Partial Bulk Transfer between registrars
    A registrar may decide to move a certain number of domain names to another registrar, e.g. linked to one gTLD because there is agreement to no longer sell domain names in the gTLD in question.
  - o Scenario III – Partial Bulk Transfer in case of a (partial) merger or acquisition between registrars
    As a result of a partial merger or acquisition between registrars, a number, but not all, domain names are transferred to the new registrar.

Marika Konings 2/5/09 8:03 PM
Deleted: 9 January 2009

Marika Konings 2/5/09 8:03 PM
Deleted: Initial

Marika Konings 2/11/09 10:27 AM
Deleted: Preliminary

Marika Konings 2/11/09 11:05 AM
Formatted: Keep with next

Marika Konings 2/11/09 10:28 AM
Deleted: It should be noted that the Working Group will not make a final decision on which solution(s), if any, to recommend to the GNSO Council before a thorough review of the comments received during the public comment period and final constituency statements has taken place.

Marika Konings 2/5/09 8:10 PM
Deleted: Initial

Marika Konings 2/5/09 8:03 PM
Deleted: 9 January 2009

Marika Konings 2/5/09 8:03 PM
Deleted: Initial

Marika Konings 2/5/09 8:10 PM
Deleted: Initial

- o Scenario IV – Partial Bulk Transfer initiated by a registrant

  A registrant decides to transfer all or a portion of his/her domain name portfolio to a new registrar, e.g. as a consequence of a merger or acquisition.

- o Scenario V – Partial Bulk Transfer following de-accreditation of a registrar

  A registrar voluntarily abandons its accreditation, and instead becomes a reseller of an accredited registrar transferring all domain names to that registrar.

- ▪ The existing bulk transfer provision reads as follow:

  "B. ICANN-Approved Transfers

  Transfer of the sponsorship of all the registrations sponsored by one Registrar as the result of (i) acquisition of that Registrar or its assets by another Registrar, or (ii) lack of accreditation of that Registrar or lack of its authorization with the Registry Operator, may be made according to the following procedure:

  (a) The gaining Registrar must be accredited by ICANN for the Registry TLD and must have in effect a Registry-Registrar Agreement with Registry Operator for the Registry TLD.

  (b) ICANN must certify in writing to Registry Operator that the transfer would promote the community interest, such as the interest in stability that may be threatened by the actual or imminent business failure of a Registrar.

  Upon satisfaction of these two conditions, Registry Operator will make the necessary one-time changes in the Registry database for no charge, for transfers involving 50,000 name registrations or fewer. If the transfer involves registrations of more than 50,000 names, Registry Operator will charge the gaining Registrar a one-time flat fee of US$ 50,000."

  Even though the current bulk transfer provisions were originally not intended to cater to the bulk transfer of domain names in only one gTLD, the Working Group recognises that the current language might provide for this option and a clarification to this end by the GNSO Council may be a useful approach. Taking this into account, the Working Group found, after in-depth discussion, that existing bulk transfer provisions and/or market solutions currently cover all scenarios.

- ▪ As a result, the Working Group does not see a need to incorporate provisions for handling partial bulk transfers between registrars at this stage.

Conclusion for Issue III

- ▪ Based on the discussion in the Working Group, having taking into account the comments received during the public comment periods and constituency statements, there appears to be broad agreement that there is no need to incorporate provisions for handling partial bulk transfers between registrars at this stage. The Working Group believes that these scenarios can be addressed either through the existing Bulk Transfer provisions, or through existing market solutions. The Working Group would recommend the GNSO Council to clarify that the current bulk transfer provisions also apply to bulk transfer of domain names in only one gTLD.

6.   Constituency Statements & Public Comment Periods

This section features issues and aspects of the IRTP Part A PDP reflected in the statements from the GNSO constituencies and comments received during the public comment period.

6.1   Initial Public Comment Period

The public comment period ran from 5 September 2008 to 29 September 2008. Three comments were received of which only one (from the IPC constituency) responded to the questions outlined in the announcement. The other two responses (from Malc McGookin and Jeffrey A. Williams) were off-topic; they expressed concerns relating to the loss of a particular domain name, the redemption grace period and warehousing. In addition, two other comments, the constituency statements of the Registrar and Registry constituency, were received after the deadline of the public comment period. The public comments on this forum are archived at http://forum.icann.org/lists/new-irtp-issues/. A summary of the constituency statements can be found in the next section.

6.2   Initial Constituency Statements

The Constituency Statement Template was sent to all the constituencies. Feedback was received from the Intellectual Property Interests Constituency, gTLD Registry Constituency, Registrar Constituency and the Business and Commercial Users' Constituency. These entities are abbreviated in the text as follows (in the order of submission of the constituency statements):

IPC - Intellectual Property Interests Constituency

RyC - gTLD Registry Constituency

RrC – Registrar Constituency

BC – Business and Commercial Users' Constituency

6.3   Constituency Views

The four statements responding to the questions outlined in the template were submitted by the Intellectual Property Constituency (IPC), the Registry Constituency (RyC) the Registrar Constituency (RC) and the Business and Commercial Users' Constituency (BC). Annex A of this report contains the full text of the constituency statements that have been submitted. These should be read in their entirety. The following section attempts to summarize key constituency views on the issues raised in the context of IRTP Part A PDP. This section also summarizes further work recommended by the various constituencies, possible actions recommended to address the three issues part of the IRTP Part A PDP, and the impact of potential measures on the GNSO constituencies.

Issue I - 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.

The IPC believes that the lack of an e-mail address for the registrant does not necessarily delay the transfer of a domain name. However, it does emphasise that if registrant e-mail address data is to be made available to other registrars, it should happen in the context of an overall technical modernization of the Whois protocol.

The RyC notes that the question might need to be restated to clarify the scope as registrant contact information such as the e-mail address is mandated in the case of thick registries; the registry operator is required to display the registrant e-mail address in the registry's WHOIS. In the case of thin registries, the RyC considers it too costly and time consuming to require thin registries to add contact information. The RyC advocates that any change to the policy should be limited to addressing the issue of obtaining authoritative information relating to the administrative contact e-mail address. In this context, a tiered access

approach to proving WHOIS information could be considered for implementation by registrars.

The RC highlights that no viable secure implementation is available which would allow registrars to make registrant e-mail address data available to one another. In addition, the RC believes the issue is more appropriate for a market based solution than for prescriptive measures.

The BC does believe a policy change is required as the current situation creates potential confusion as 'the Admin Contact email address is purportedly authoritative, yet can be overruled by a Registrant'. The BC suggests that a potential solution could be to make the Admin Contact email address authoritative for a transfer and in addition employ authentication technologies to authenticate transfer requests and acknowlegments.

Issue II - 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).

The IPC believes that there is a need for further options for electronic authentication in order to set a reasonable secure and basic standard to be used by every registrar, and that such options should be independent of any other services offered by the registrar. However, such a system should improve security without making the transfer process too cumbersome. Possible solutions could include the requirement for the registrant to submit with its request to unlock the name the IANA ID of the Gaining Registrar or the use of digital certificates. The IPC believes that an analysis of various ccTLD registry policies such as the Swedish registry (.se), the Swiss registry (.ch) and CoCCA (.cx, .mu, .na, etc), would benefit the policy development process. The IPC does recognize that unexpected and increased costs for registrants or at the registry level could be an issue.

The RyC supports the principle that market forces should handle this issue; registrars are best placed to measure demand and decide whether they would like to differentiate themselves from their competitors by making additional security measures available for their

customers. The RyC has identified a number of registrars that provide such additional security methods to their customers such as Markmonitor, GoDaddy and Moniker. However, if a need would be identified for other options of electronic authentication, the RyC recommends that the EPP AuthInfo code be explored in further detail as this mechanism already provides an automated way to authenticate transfer requests and could take the place of both the Registrant and Admin contact e-mail addresses. The RyC notes that for the use of AuthInfo codes to be effective, compliance with the requirement that AuthInfo codes be unique by domain name must be enforced via the ICANN Registrar Compliance Program and not the registry operator.

The RC also recommends that this issue be resolved based on market demand rather than prescriptive measures and cautions against unintended consequences of technology mandates.

The BC does believe there is a need for other options for electronic authentication such as PGP or other authentication methods. In addition, it calls upon SSAC, GNSO and other ICANN bodies to continue working to investigate and mitigate the risk of domain name hijacking.

Issue III - 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.

The IPC believes that the transfer policy should incorporate provisions for handling partial bulk transfers. It considers it particularly helpful in the context of corporate asset sales and acquisitions in the context of a registrant or in case of the termination or non-renewal of a registrar's accreditation agreement.

The RyC supports the incorporation of provisions to handle partial bulk transfers as long as this would not require reengineering the existing bulk transfer functionality or new development. Specific details of the product offerings by registries and registrars should be left to the market.

The RC also believes that a partial bulk transfer option would be a useful tool for registrars, as long as it is properly defined. It does note that many details still need to be refined such as 'how many domain names constitute a bulk transfer' before a policy can be considered in this area. It emphasizes that such a policy should be limited to partial bulk transfers between registrars; partial bulk transfers for registrants should be left to market-driven innovation and competition.

The BC supports that there should be such a provision to allow large domain portfolio owners to transfer large chunks of domain names between registrars; provisions to facilitate partial bulk transfers should not be limited to registrars only.

6.4   Initial Report Public Comment Period

The comment period ran from 9 January 2008 to 30 January 2009. Four comments were received of which three commented on the Initial Report (Patrick Mevzek, Barbara Steele on behalf of VeriSign and Clarke Walton on behalf of the Registrar Constituency). The other comment (from Thom Baird) related to a problem with the transfer of a particular domain name. The following section attempts to summarize the relevant comments received. Annex contains the full text of the relevant comments received.

Summary

Patrick Mevzek submitted his comments as an individual generic Internet user, owner of some domain names for personal and business needs, a founder of a company working with ICANN registries, registrars, and domain name providers, a participant in IETF Working groups related to EPP & IRIS and creator of software implementing both EPP and IRIS. Mevzek provided comments on all three issues outlined in the Initial Report. As a general comment he noted that there is a 'need to find a middle ground between the ease of transfer to make sure no arbitrary registrar locking can take place on the one side and on the other side enough guarantees that only legitimate transfer requests happen and succeed. He questioned whether sufficient data currently exists to assess which, if any, problems exist

---

with the current transfer policy and noted that other data on transfers might be helpful 'so that policy procedures and energies can be properly spent depending on hard facts'. Nevertheless, he considers improvements welcome as long as the current situation is taken into account 'before providing too much new requirements in policies or new software developments'.

In relation to issue I, the potential exchange of registrant e-mail information, Mevzek comments that he does not support the idea of the poll mechanism of EPP to be used to transfer messages between registrars. He noted that 'it was not intended this way in the protocol'. He also highlights that if the current EPP system would be used for this purpose a number of 'security and denial of services potential problems' might emerge, 'not even thinking about the new specifications that would needed to be written, [and] then the new software development at both registries and registrars!'. In Mevzek's view, IRIS would be the most appropriate solution for transmitting data between registrars and/or registries in a secure manner, including traceability and authentication. Mevzek does note that this would imply that every registrar would need an IRIS server, which might be an unrealistic goal. Instead, he notes that 'a shortcut could be achieved in thick registries, as only a registry IRIS server would be needed, available only to registrars'. He also notes that costs and time to implement a new technique should not act as a deterrent if no other means are available to address a problem. On the registrant vs. admin approval issue, Mevzek notes that in his view 'both parties should remain involved in the process, they should have the same rights regarding initiating, confirming or declining a transfer'. On the AuthInfo code, he does not think it would make sense to 'add this new requirement of authinfo code to the older one'. In addition to commenting on the different options discussed by the Working Group, Mevzek puts forward a number of ideas for consideration by the Working Group:

- 'The EPP protocol has a domain:info operation which reveals all data related to the domain, including the contact IDs of the registrant. This operation accept[s] an authInfo code, the idea being that if the registrar doing it is not the current sponsoring registrar of the domain name, it might still get information on it if it has the proper authInfocode'. He does note that this would require a policy change as currently 'some registries allow domain:info done by all registrars and some do not'. He goes on noting that 'the

Marika Konings 2/5/09 8:41 PM
Formatted: Line spacing: 1.5 lines
Marika Konings 2/5/09 8:37 PM
Formatted: Bullets and Numbering
Marika Konings 2/5/09 8:10 PM
Deleted: Initial
Draft Final Report on IRTP Part A PDP
Author: Marika Konings
Page 32 of 82

contact:info operation works basically the same way […] with an optional AuthInfo', but a small issue might be that this is a different AuthInfo code than the one used in the domain:info operation. According to Mevzek, this issue could be resolved in a number of ways such as disclosure of the contact AuthInfo, change of contacts and changing the AuthInfo structure for the contact. He notes that this option would 'need only minor technical specification […] and very little changes in current software both on registrar and registry sides'.

- 'The transfer policy could be simplified a lot and at the same time this issue could be resolved if the policy is changed so that it requires **only** the AuthInfo code to start the transfer, removing the contacts email handling. The current sponsoring registrar would still be allowed to notify contacts and would be allowed to stop the transfer if one of the contacts says so'. Mevzek notes that he does not understand the concern raised by the Working Group in this regard as not being a 'secure and viable solution compared to the current system'.

This last solution has Mevzek's preference. However, he indicates that if such a change in policy would not be possible, he would 'recommend working on making the registrant contact a same class citizen as the administrative one and maybe taking it out of the equation […] and at the same time working either on IRIS and/or EPP […] to see how exchanges of email addresses could be made simpler or exchanged for other authentication, based on the current authInfo'.

On issue II, the potential need for other options for electronic authentication, Mevzek wonders why emails 'are still used as primarily token of authentication during domain transfers, in contrast of using the more secure AuthInfo one'. He highlights a number of ideas such as protection of email by openPGP and/or S/MIME and access to a website using SSL certification as options to could be explored. However, he does emphasize that he does not think that 'the GNSO/ICANN should start defining these mechanisms […] that would apply uniformly to each registrar'. In his view, it should be up to registrars to decide 'if they want to use other methods of authentication, and which ones'. As a suggestion, he proposes that ICANN 'could monitor which mechanisms are used by registrars and verify they meet some requirements'.

On issue III, the potential need for provisions for handling partial bulk transfers between registrars, Mevzek again notes that it would be helpful to have further data on this issue to guide the discussion. After having reviewed the different scenarios outlined by the Working Group, he agrees with its conclusion that 'there is no need to incorporate provisions for handling partial bulk transfers between registrars at this stage'.

Barbara Steele submitted her comments on the three issues on behalf of VeriSign to the public comment forum. On issue I, the potential need for exchange of registrant email information between registrars, VeriSign notes that 'the majority of Registry Operators that maintain thick Whois information are contractually required to make the registrant e-mail address publicly available'. It recommends that 'further discussion should occur to determine why this is a requirement for some thick Registry Operators but not all and it is not a requirement for any Registrars'. VeriSign expresses concern in relation to the time and costs of the different options discussed by the Working Group. VeriSign comments that it does not consider any future discussion on a potential policy change which would prevent the registrant from reversing a transfer appropriate as it 'could make it easier for a domain name to be hi-jacked'.

On issue II, the potential need for other options for electronic authentication, VeriSign notes that other options for electronic authentication 'may be helpful', but that it 'should be left up to the registrar to choose whether or not to provide as a part of its offering'.

On issue III, the potential need for provisions for handling partial bulk transfers between registrars, VeriSign 'agrees that market solutions should be the preferred method for addressing this issue'.

Clarke Walton submitted the position of the Registrar Constituency (RC) to the public comment forum. It should be noted that due to time constraints, no formal vote was taking on this position paper by the RC. In comparison to the position submitted on 3 October 2008, which is also included in the Initial Report, the position paper notes that RC has only revised its view on Issue III in response to the conclusions reached by the Working Group in its Initial Report.

On issue I, the potential exchange of registrant email information between registrars, the RC 'believes that regulatory intervention is not necessary to address this issue' as it is 'more appropriate for market based solutions'. The RC does recommend further consideration of the issue of the Registrant's authority to overrule the Admin contact in future IRTP PDPs.

On issue II, the potential need for other options for electronic authentication, the RC supports that this issue is left to market demands instead of regulation.

On issue III, the potential need for provisions for handling partial bulk transfers between registrars, the RC supports the conclusions of the Working Group that at this stage there is no need for specific provisions for handling partial bulk transfers.

Conclusion

In relation to issue I, the potential exchange of registrant email information between registrars, one comment (the Registrar Constituency) does not see a need for policy development in this area as it is of the opinion that this should be left to market based solutions (RC). A second comment (VeriSign) does recommend further discussion on the requirement for some thick registries to make registrant email information available, but does express concern over the time and costs involved in the different options discussed by the Working Group. The third comment (Peter Mevzek) does see possibilities to address this issue via IRIS, the domain:info / contact:info operation or changes which would make the AuthInfo code the only authorization for a transfer.

On issue II, the potential need for other options for electronic authentication, all comments received agree that this should be left to market based solutions.

On issue III, the potential need for provisions for handling partial bulk transfers between registrars, all comments received agree with the preliminary conclusions of the Working Group that there is currently no need for specific provisions for handling partial bulk transfers.

7. Conclusions and Next Steps

Based on the discussion in the Working Group, having taking into account the comments received during the public comment periods and constituency statements, the Working Group concludes the following.

Conclusion for Issue I - 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.

- The WG noted that WHOIS was not designed to support many of the ways in which it is currently used to facilitate transfers. Some members suggested that finding a way to make the Registrant e-mail address more readily available could be addressed as part of an overall technical modernization of the WHOIS protocol. This could be through updates to the existing protocol, modification of the Extensible Provisioning Protocol (EPP) or adoption of the Internet Registry Information Service (IRIS) protocol. However, after review and discussion none of these options received broad agreement.

  The WG did note that, in the absence of a simple and secure solution for providing the gaining registrar access to the registrant email address, future IRTP working groups should consider the appropriateness of a policy change that would prevent a registrant from reversing a transfer after it has been completed and authorized by the admin contact. This option would not change the current situation whereby a losing registrar can choose to notify the registrant and provide an opportunity to cancel a transfer before the process is completed.

Conclusion for Issue II - 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).

- Based on the discussion in the Working Group, having taking into account the comments received during the public comment periods and constituency statements, there appears to be broad agreement that there is a need for other options for electronic authentication. However, opinions in the Working Group differ as to whether these options should be developed by means of GNSO policymaking or should be left to market solutions.

Conclusion for Issue III- 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.

- Based on the discussion in the Working Group, having taking into account the comments received during the public comment periods and constituency statements, there appears to be broad agreement that there is no need to incorporate provisions for handling partial bulk transfers between registrars at this stage. The Working Group believes that these scenarios can be addressed either through the existing Bulk Transfer provisions, or through existing market solutions. The Working Group would recommend the GNSO Council to clarify that the current bulk transfer provisions also apply to bulk transfer of domain names in only one gTLD.

The Final Report is a step in the GNSO Policy Development Process and a basis for further deliberations in a next step. The report is based on the Initial Report that has been posted for public comment for 20 days as prescribed by the ICANN bylaws (see http://www.icann.org/general/bylaws.htm#AnnexA). Public comments submitted have been incorporated by ICANN staff into this Final Report, which is submitted to the GNSO Council. The Final Report (along with the preceding Issues Report) will serve as a basis for subsequent deliberations and actions by the GNSO Council in formulating recommendations to the ICANN Board regarding changes, if any, that should be made to the inter-registrar transfer policy in relation to the issues covered by this PDP.

Annex A – Template for Constituency Statements

Constituency Input Template Inter-Registrar Transfer Policy Set A

The GNSO Council has formed a Working Group of interested stakeholders and Constituency representatives, to collaborate broadly with knowledgeable individuals and organizations, in order to develop potential policy options to address three new issues associated with the Inter-Registrar Transfer Policy.

Part of the working group's effort will incorporate ideas and suggestions gathered from Constituencies through this Constituency Statement.

Inserting your Constituency's response in this form will make it much easier for the Working Group to summarize the Constituency responses. This information is helpful to the community in understanding the points of view of various stakeholders.

For further background information on this issue, please review the GNSO Issues Report on Inter-Registrar Transfer Policy Set A - New IRTP Issues

Process:
• Please identify the members of your constituency who participated in developing the perspective(s) set forth below.
• Please describe the process by which your constituency arrived at the perspective(s) set forth below.

Issue I – 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.

- 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.

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

Issue II – 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).

- 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.
- Do you think there is a need for other options for electronic authentication? Please state the reasons for your answer.
- 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?
- If a need would be identified for other options of electronic authentication, what other options could be explored?
- Of those other options to be explored, please identify the potential benefits but also any potential problems.
- 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.

- 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?

Issue III – 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.

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

Marika Konings 2/5/09 8:03 PM
Deleted: 9 January 2009

Marika Konings 2/5/09 8:03 PM
Deleted: Initial

Marika Konings 2/5/09 8:10 PM
Deleted: Initial

Marika Konings 2/5/09 8:03 PM
Formatted: Bullets and Numbering

Annex B - Constituency Statements

IPC Comments On Inter-Registrar Transfer Policy (IRTP) Issues
Part A 'New IRTP Issues'
September 26, 2008

Issue I - 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.

COMMENTS

The lack of an e-mail address for the Registrant generally does not delay the transfer of domain registrations, for the simple reason that, to our knowledge, when the Admin Contact e-mail is functioning, no registrar even attempts to obtain approval by any other means. In most cases, furthermore, the Registrant or an authorized employee's e-mail address is listed as the Admin Contact, so the Registrant in fact consents to the transfer. Nevertheless, the value judgment implicit in the Issue - that it would be preferable to be certain that the entity listed as the Registrant consents to the transfer - is sound. In cases where the Registrant and the Admin Contact are not the same, it seems plausible that confusion could result over whether the Registrant actually consented to a transfer, or whether a Registrant's purported authorization (or rejection) of a transfer from an e-mail address not listed in the Whois was authentic.

However, if Registrant E-mail Address data is to be made available to other registrars, it should happen in the context of Whois. One purpose of the Port 43 protocol was to provide information necessary for inter-registrar transfers, so developing a separate protocol to provide certain pieces of information necessary to that process would be superfluous. If

Registrant E-mail Address data is to be made available, it should be done as part of an overall technical modernization of the Whois protocol.

The need for inter-registrar communication of registrant information speaks to the legitimate need for Port 43-like access to Whois data (in addition to the public's need and the need of intellectual property owners for open access to Whois data, such as can be obtained through web interfaces). Other parties with needs for Port 43-like automated access include information providers, such as those who provide research services for non-marketing purposes such as trademark availability clearance and searching, audits of domain portfolios for corporate mergers and acquisitions, and investigations of intellectual property infringement and fraud. The need for Registrant E-mail Address data in Whois is just one of many reasons why ICANN should address, rather than avoid the need to modernize the Whois protocol.

Issue II - 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).

COMMENTS

Yes, we believe that there is a need for further options for electronic authentication in order to set a reasonable secure and basic standard to be used by every registrar, and that such options should be independent of any other services offered by the registrar. It is important that ICANN sets out the requirements for this basic standard in its IRTP. The challenge is to find a way to improve security without making the transfer system too cumbersome.

The weakness in almost every current system for electronic authentication is that too much depends on information and confirmation via e-mail (of the registrant's and/or the Admin Contact). Even with partial off-line authentications (e.g. in the form of a signed fax from the Registrant) in combination with an e-mail confirmation, it is necessary to rely on the presumption that the registrant's e-mail address is correct because any additional documentation requiring signature is sent via that e-mail address.

Marika Konings 2/5/09 8:03 PM
Deleted: 9 January 2009

Marika Konings 2/5/09 8:03 PM
Deleted: Initial

Email-based authentication does not appear to be sufficient to secure the identity of the registrant.

A current risk point is that there is a period after a registrant has unlocked a domain name during which malicious transfer requests might accidentally be accepted. One possible solution could be to require the registrant to submit with its request to unlock the name the IANA ID of the registrar to which the name is intended to be transferred. Transfer requests coming from any other registrar would then be automatically rejected.   Another solution is the use of digital certificates.

However, we appreciate that certain registrants and certain areas of business - the financial sector, for example - may require an even higher standard and level of security. We see these classes of registrants and business sectors are best served by additional services that are created and offered by the registrars without involvement of ICANN.

The IPC believes an analysis of various ccTLD registry policies would benefit the policy development process. Examples include the Swedish registry system which uses an application called Domain Manager ('DomÃnhanteraren'), and features a certificate-based web interface to effectuate transfers. In the Swiss Registry (SWITCH), authentications are performed either via e-mail or by signed fax only. CoCCA (a grouping of small ccTLD registries) uses a password generated by electronic token for allowing access to the registrar account, but does not authenticate a registrant's right to a transfer.

The benefits of improved electronic authentication are safer communications and transfers. Potential problems could be unexpected and increased costs for Registrants - either by demands for certain software or by increased costs at the Registry level (which will ultimately raise the price for domain name administration), as well as a more time-consuming process whenever a certification of the Registrant's ID is needed.

Issue III - 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.

Marika Konings 2/5/09 8:10 PM
Deleted: Initial

COMMENTS

Yes, the policy should incorporate provisions for handling partial bulk transfers. Any mechanism to facilitate the smooth transfer of a registrant's domain names is welcomed. Partial bulk transfers would be particularly helpful in connection with corporate asset sales and acquisitions. For example, a registrant may be selling only one of its business lines to a third party or an acquiring company may wish to have only some of the acquired company's domain names transferred to its own registrar. Furthermore, in the cases of termination or non-renewal of a registrar's Registrar Accreditation Agreement, a partial bulk transfer policy would enable the de-accredited registrar to transfer domains in bulk to numerous 'gaining' registrars, further protecting the rights of registrants.

Submitted by,

Claudio DiGangi, on behalf of IPC

Marika Konings 2/5/09 8:10 PM
Deleted: Initial

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[5]: 15
- Total # of RyC Members: 15
- Total # of Active RyC Members[6]: 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)

---

[5] 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 .
[6] 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.

- Names & email addresses for points of contact

o Chair: David Maher, dmaher@pir.org

o Vice Chair: Jeff Neuman, Jeff.Neuman@Neustar.us

o Secretariat: Cherie Stubbs, Cherstubbs@aol.com

o 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 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.**

   2.1 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.

   2.1.1. 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.

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

2.2.1. 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.

2.3 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.

2.3.1. 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.

2.3.1.   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.

October 3, 2008

Registrar Constituency Position on Inter-Registrar Transfer Policy Issues

BACKGROUND

In September 2008, the Registrar Constituency ("RC") was asked to provide feedback regarding three Inter-Registrar Transfer Policy ("IRTP") issues. This Position Paper captures the overall sentiment expressed by the RC Members who provided feedback about this matter and seems to reflect the general sense of the RC. Due to time constraints, however, no formal vote regarding this Position Paper was taken.

RC POSITION

The RC's position regarding each of the three IRTP issues is as follows:

1. Is there a way for registrars to make Registrant E-mail Address data available to one another?

No viable secure implementation of this proposal has been advanced that would enable a policy to require registrars to make Registrant E-mail Address data available to one another. Additionally, the RC believes that regulatory intervention is not necessary to address this issue. This issue is more appropriate for market based solutions rather than regulatory intervention.

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).

The RC does not believe that a regulatory approach to authentication is necessary. The RC recommends that the questions of whether additional authentication technology is needed, and if so which technology to implement, be decided based on market demands rather than regulation.

To that end, the RC cautions ICANN about the unintended consequences of technology directives. Specifically, any mandated technology is guaranteed to become the target of hackers who seek to circumvent its security. Having the option of a variety of technologies which may be developed and implemented based on market demands offers greater security in the long-run.

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.

The RC believes that, properly defined, a "partial bulk transfer" option would be a useful tool for registrars.

There are at least three scenarios in which this option may be helpful to registrars, including:
• A private business transaction between registrars, in which a subset of the domains / customers from one registrar are transferred to the other;
• A registrar's reseller becomes an accredited registrar, and seeks to change the registrar of record at the registry; or
• A registrar discontinues retail registrations in a given TLD, or is involuntarily deaccredited by ICANN.

However, many questions remain unanswered. For example, the RC questions how many domain names would constitute a "bulk" transfer. Also, does the term "partial" indicate that the losing registrar would maintain some remaining registrations in the TLD? Furthermore, what is the method for assessing fees? Should this be a flat fee, or sliding scale? Should an additional registration year be included or omitted from the transfer?

Also, the RC opposes any recommendations or language that extends this option to registrant-initiated transfers for large portfolio holders on the basis that this is better characterized as product development, not policy development. A consensus policy would not take into account the variety of registrar business models, and would impose the same terms, restrictions and limitations on all registrars regardless of its applicability to their

customers. Additionally, there are several services available now that address this need.

The RC suggests that ICANN continue to let market-driven innovation and competition address the needs of registrants who manage large domain name portfolios, and limit the discussion of partial bulk transfers to situations arising "between registrars."

CONCLUSION

The opinions expressed by the RC in this Position Paper should not be interpreted to reflect the individual opinion of any particular RC member.

BC Constituency Statement

Constituency Input Template Inter-Registrar Transfer Policy Set A

The GNSO Council has formed a Working Group of interested stakeholders and Constituency representatives, to collaborate broadly with knowledgeable individuals and organizations, in order to develop potential policy options to address three new issues associated with the Inter-Registrar Transfer Policy.

Part of the working group's effort will incorporate ideas and suggestions gathered from Constituencies through this Constituency Statement.

Inserting your Constituency's response in this form will make it much easier for the Working Group to summarize the Constituency responses. This information is helpful to the community in understanding the points of view of various stakeholders.

For further background information on this issue, please review the GNSO Issues Report on Inter-Registrar Transfer Policy Set A - New IRTP Issues

Process:

• Please identify the members of your constituency who participated in developing the perspective(s) set forth below.

Mike Rodenbaugh, Rodenbaugh Law

Michael Collins, Internet Commerce Association

Mike O'Connor, The O'Connor Company

• Please describe the process by which your constituency arrived at the perspective(s) set forth below.

This request for input was circulated for comment from BC Members on two occasions. A draft response was created by Mike Rodenbaugh and circulated for comment. This final draft was submitted.

Issue I – 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.

• 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.

BC: We believe policy change is needed. The current system is inconsistent and insecure. The Admin Contact email address is purportedly authoritative, yet can be overruled by a Registrant who need not even provide an email address. Buyers of domain names need better assurance that they are purchasing from an authorized seller, this has been an important function of the WHOIS database since the Admin Contact email address can be verified by a buyer. The buyer has no way of knowing, however, if there is a superior registrant who can disrupt the transaction.

Yet today, this situation also seems to provide a security layer because registrars often have Registrant email addresss and other contact info that is not public in WHOIS, and they can use this information to confirm suspicious transfers. This may be a security benefit, but also causes confusion. We should find a way to increase security and decrease confusion.

One answer may be to further clarify that the Admin Contact email address is authoritative, and consent from that address is assurance for a legitimate transfer that cannot be undone by the prior registrant. In that event, PGP or some other authentication method should be deployed to authenticate transfer requests and acknowledgments, because traditional email is blatantly insecure and easily spoofed.

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

• 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.

BC: We think the above solution, making the Admin Contact clearly authoritative, is a better solution than to add another piece of contact data to the WHOIS database. The Registrant email address could be different from the Admin Contact email and thereby create confusion as to which is authoritative.

Issue II – 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).

• 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.

BC: It is a frightening risk that important domain names can be hijacked via email spoofing, hacking and otherwise. There are countless ways in which businesses and their users can be harmed financially, reputationally and even physically when a critical domain is overtaken by hostile and/or criminal actors. We encourage SSAC, GNSO and other ICANN bodies to continue working to investigate and mitigate this risk.

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

BC: Yes. Traditional email is inherently insecure. Some domain names are critical for business and government infrastructure, and it is proven that they can be hijacked. PGP or other authentication methods could be devised to impose minimal burden on registrants or registrars, yet ensure much more effective security than is standard today.

- 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?

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

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

- 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.

- 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?

Issue III – 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.

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

BC: Yes. Large domain portfolio owners should have freedom and ability to move large blocks of domains freely among registrars. Today, some registrars make the transfer process difficult or impossible to do in bulk, and there is much inconsistency among the various registrars. There ought to be a standard mechanism for large portfolio owners to move large blocks of names among registrars. It would be particularly disturbing if the registrars were to have such a policy for partial bulk transfers among themselves, but did not offer that functionality to bulk registrants.
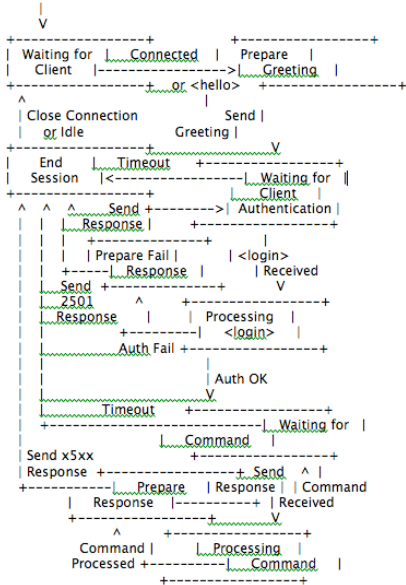

- Are you aware of any voluntary provisions to facilitate partial bulk transfers? If so, could you please provide further details on those provisions (apart from those already identified in the issues paper – NeuLevel (.biz), Nominet (.uk)).

Annex C – EPP

What is EPP?

```
            |
            V
+------------------+          +------------------+
| Waiting for      |_Connected|    Prepare       |
|   Client         |---------------->|  Greeting |
+------------------+    or <hello>   +------------------+------+
        ^                      |
        | Close Connection          Send |
        | or Idle            Greeting |
+------------------+              +------+
|   End            |  Timeout    +------------------+
| Session          |<----------------|  Waiting for  ||
+------------------+              |     Client      |
  ^  ^  ^   Send +-------->| Authentication |
  |  |  |  Response |      +------------------+
  |  |  +------------+     |
  |  |  | Prepare Fail |   | <login>
  |  |  +-----| Response |  | Received
  | Send +----------------+   V
  | 2501        ^      +------------------+
  | Response    |      |   Processing     |
  |          +---------+  | <login>      |
  |       Auth Fail +------------------+
  |              |
  |              | Auth OK
  |              V
  |   Timeout  +------------------+
  |----------|  Waiting for     |
  |          |   Command        |
  | Send x5xx  +------------------+
| Response +------------------+  Send  ^ |
+----------- Prepare | Response | Command
  |   Response  |----------+ | Received
  +---------------+        V
            ^      +------------------+
  Command |      |   Processing     |
Processed +---------|   Command      |
            +------------------+
```

Source: http://www.ietf.org/rfc/rfc4930.txt

Annex D – Initial Report Public Comments

   * To: irtp-initial-report@xxxxxxxxx
   * Subject: Comments on irtp-a-initial-report-08jan09.pdf
   * From: Patrick Mevzek <contact@xxxxxxxxxxxxx>
   * Date: Thu, 29 Jan 2009 03:15:57 +0100

Please find below some of my comments on the document irtp-a-initial-report-08jan09.pdf
I'm writing these comments as an individual generic Internet user, owner of some domain names for personal and business needs, a founder of a company working with ICANN registries, registrars, and domain names providers, a participant in IETF Working groups related to EPP & IRIS, and creator of software implementing both EPP and IRIS.
Of course, I'm only speaking for myself.

===

Executive summary of my comments below:

- Issue 1: IRIS is probably the best road ahead, but some work on EPP may help too (but probably not on poll messages as offered in the report), where a major change in policy (enforcing the authinfo as the true only primarily token of authentication) would even have my preference over any technical change. I give some other specific ideas below.
- Issue 2: I mostly agree with the report preliminary conclusion, but I would favor more market free innovation to define new ways of doing authentication, with some policy safeguards.
- Issue 3: I absolutely agree with the report preliminary conclusion.

I praise the working group for having been able, specially for issue 1, to take into account so many different ways that may help to reach a solution, both on technical and policies grounds. This is a very good effort and work, that I applaud.

==

Introduction to my comments on all 3 issues below.

Domain name transfers (like whois) have always been an outstanding issue, between technological changes (such as the introduction of EPP and its "authcode"), policy changes (like http://www.icann.org/en/transfers/policy-12jul04.htm), new attacks and "famous" thefts (true or alleged).

Policies and processes need to find a middle ground between the ease of transfer to make sure no arbitrary registrar locking can take place on one side and on the other side enough guarantees that only legitimate transfer requests happen and succeed.

Before starting to directly answer the 3 issues presented, I would like to say that based on the only public data I know (the ICANN registries monthly reports as PDF), there does not seem to be a lot of problems with transfers.
I've used the monthly reports PDF to tabulate data in other ways and create graphs, and you can see them on my website at http://www.testing.dotandco.net/ressources/icann_registries/index.en and for example on .COM transfers:
http://www.testing.dotandco.net/ressources/icann_registries/verisign_com_net/transfers_COM.en

If there is other data on transfers, it would be good to know them, so that policy procedures and energies can be properly spent depending on hard facts.

If you look at the above transfers numbers you come to the conclusion that failed transfers are low, often around or below 5% (with .COM being higher than that but this is pretty much to be expected, based on the number of .COM domain names and the image of .COM, a gTLD better known than any other one). This does not mean there are as much problems, as transfers can fail for a myriad of valid reason such as: error from the registrant (not

---

transfering the correct domain names, or not at the appropriate time), from the current sponsoring registrar or the prospective one.
Sadly, there is no way, nor requirement, for the registry and the current sponsoring registrar to document why they reject a transfer (no provision for that in EPP), so there is no data that show which cases among the list of 9 points in §3 of http://www.icann.org/en/transfers/policy-12jul04.htm explains why transfers have been refused.

A number that may be even more revealing, is the one about transfer disputes, and its spread between disputes that has been solved (in favor of one of the two registrars involved) and disputes without decision (per the process specified at http://www.icann.org/en/transfers/dispute-policy-12jul04.htm) This number is very low, often less than 10 disputes per month. This does not cover all kind of possible disputes, as disputes handled outside of the registry operator are probably not computed there, nor are all disputes handled by courts around the world, but I doubt that the numbers would change a lot if they would be all counted.

Which means to me that the current system do seem to work "good enough". It does not mean that effort should not be spent toward improving it even more, but the current situation should be taken into account before providing too much new requirements in policies or new software developements.

==

Issue 1. Potential exchange of registrant e-mail information

I think part of the problem comes from the fact that the registrant "contact" is handled differently than other contacts (administrative, billing, technical), where today this difference makes no sense at all.

If, in the past (more than 10 years ago), people were owner of domain names without maybe even knowing anything about the internet (so not necessarily having an email

address), and thus giving their authority to the admin contact that acted on their behalf, I doubt that this situation is prevalent today. So, in all policies documents and thus technical procedures, all 4 types of contacts should be handled exactly the same way, with the same requirements on what data needs to be provided, how it is used, and so on. The email address should be there for all contacts, and displayed/used the same way. See for example the Registrar Data Escrow Requirements, where emails of all contacts are to be dumped... except for the registrant ones! And for whois display. (I do observe however in some quick tests that registrant email address is displayed in whois for AERO ORG INFO BIZ MOBI CAT TRAVEL at least; since .COM/.NET are thin it depends on each registrar) But whois display cross the issues of personal information in whois, and this is another debate.

The registry implication do vary also because it depends on its status, as thin or thick registry. Any work today on these issues should take into account current TLDs but also forthcoming ones, and I have personnaly no idea/information if future registries will be thick or thin, even if all the latest additions were thick ones.

This issue 1. asks if there is a way for registrars to make registrant emails data available to one another. Before giving some ideas of my own, I would like to comment on points given in the report presented (pages 15 and following).

- EPP : I do not believe the poll mechanism should be used to transfer messages between registrars. It was not intended this way in the protocol (and specifically, some registries in the world based on EPP dislike the idea of poll messages, and started their business without it ; some have added poll messages some not ; it just shows that poll messages are an EPP feature on which there is no absolute consensus), as it is purely a channel for the registry to *asynchronously* inform the registrars on some information. Allowing registrars (client side of EPP) to create messages, and even allowing them to choose the destination (the other registrar, which would need to be identified) of messages seem to me very unnatural in the current EPP specifications, and an horror waiting to happen due to security and denial of services potential problems, not even thinking about the new specifications that would needed to be written, in then the new software developement at both registries and

registrars! This whould be a huge amount of work to shoehorn something like that where there is another solution that fits more naturally, IRIS.

- IRIS : IRIS is the successor of whois... except the only fact that is not used anywhere today publicly (except for something closer to a domain availability check then a whois, in .DE) . It has however two major points that are a mess today in whois:
* a clear format (based on XML), where whois lacks any standardized format at all
* a core mechanism to handle authentication and authorization policies, where there is none in whois.

If any data should be transmitted between registrars and/or registries securely, with traceability and authentication, in my view, IRIS would be the solution.

However, it would mean having an IRIS server working at each registrar. This may seem unrealistic as they are already problems with registrars whois servers, at least some of them, from time to time. So making a new technical developement mandatory to something like 1000 registrars is not a guarantee to achieve it in a reasonable time I'm afraid. A shortcut could be achieved in thick registries, as only a registry IRIS server would be needed, available only to registrars.

But I would like to pinpoint something: having the need to do some software development should not be taken as an argument against some solution. Innovative and new services pretty much always need new developement to start with, and anyway, IRIS should be something pursued in the future in other cases, like the current complete mess with all whois issues (while at their core these issues are not technical and hence can not be solved only with technical changes, this does not mean that new technical solutions could not help, together with policies and procedures, to achieve a better state). So, if there are two solutions for a problem, and one requires new technical development while others do not, then we may say that the one without software development should be prefered. However if this solution does not exist, and the only one or the best one do require some technical development, then it should not be an argument against it. Of course the related costs and

time to market should be taken into account, but by itself this should not eliminate the solution in question from being studied.

No solution should be based on working on the current whois system, and if that happens, this should be changed to work on IRIS solutions to replace/enhance the current whois.

- Registrant vs admin approval : I believe that if both parties should remain involved in the process, they should have the same rights regarding initiating, confirming or declining a transfer.
If they do not have or can not have the same rights and tools to act upon transfers (or other areas for that matter), then only one party should remain, and the other should not intervene anymore in the process.

However, as outlined above, since these 2 entities are not handled the same way currently, it would be a problem to choose one over the other.

I also fear that choosing one over the other, makes the loosing one almost worthless, at least on the registry level (registrar are free to use their authorization system locally in any way they see fit based on contacts and their appropriate passwords; along the road, I would like to share my experience on that stating that not all EPP registries worldwide use the same set of contacts - some do not use the billing one, some do use other ones - and also that EPP allows on the protocol level to have multiple contacts of the same types for a domain name, like having 3 administrative contacts ; this last point - even if not really seen today - may create the exact same problem as this issue is trying to solve with more than one actor).

I would however slightly prefer, if this is the solution taken, to favor the administrative contact over the registrant because, first it is the current system and it solves the problem of having to get the registrant email which would not be needed in anyway as the registrant would not intervene at all, and second because I think we are in either of these two cases:

---

* some entity, for various normal reasons, wishes to own domain names, but let some other company (one of its affiliates, its lawyers, its webhosting company or technical provider, etc.) manages them ; they thus would be registrant, but the other entity would be the admin contact (and probably also the technical/billing one is many cases). In this situation, all operations on the domain name are conducted by the admin contact, so the registrant should not be participating at all, as it clearly stated (by not being the admin contact itself) that some other entity has the right to act on its behalf for domain name management

* or some entity wants to own domain names and manage them, maybe while leaving only technical stuff (like DNS management) to some outside company, which would be the technical contact only. In this case this entity would be at the same time the registrant and admin contact.

So if we take into account these two cases, dealing with the admin contact only should be enough and the proper way to manage a transfer.

As I'm sure to have forgotten some other cases, I'm not sure however that such a clear cut would be always possible and siding with the admin contact. If they are however no other cases, using only the admin contact should seem reasonable.

For uniformity, I would recommend in all cases, that if the registrant is taken out of the equation on the new registrar round of contact emailing to get transfer authorization, then it should also be taken out of the current sponsoring registrar round of (optional) contact emailing, in order to avoid very difficult cases to understand. So basically : the new registrar emails the admin contact (after having been given the authinfo code) and proceeds with the transfer if it gets express positive agreement from admin contact, the transfer is started, and if the current sponsoring registrar wishes to double confirm, it emails only the admin contact, and stop the transfer only with an express negative reply. At least, this would be my advise.

- AuthInfo code : this is an interesting point related to the way EPP was created.
EPP was created after transfers started to happen in gTLDs. EPP was created with an idea of using authInfo to start a transfer, in such a way as the simple possession of the authInfo

token means the acting party (the new registrar on behalf of "someone" that gave him the authinfo, and that someone must have been authorized in some way by the previous authinfo to get this code) has all necessary proof it is currently making a legit transfer request, and not a bogus one.

When EPP came in production, the current set of policies regarding transfers were modified to take into account this new token of authentication. By then transfer policies already had the mechanisms with emailing the contacts and waiting for their acknowledgment, albeit without any clear standardization of messages or procedure flow. But EPP AuthInfo was then added to the current policies, as an additionnal step, without reframing the policies themselves.

However in my mind as a software developer regarding EPP, its authinfo mechanism should then have been used instead of the current system with contact emails and acknowledgments. Of course care would need to be taken into account to ensure proper transition over to EPP, as oldest registries were still using RRP. Introduction of authInfo created many problems, because it was something new and not very well understood by a large proportion of registrars (which lead to various problems such as the same authinfo used for all domain names, refusal to give the authinfo and thus blocking outgoing transfers, and so on...) But, again, as an EPP technical specifications participant and later developer, it makes low sense to add this new requirement of authinfo code to the older one. It should be one or the other, not both. And since the authInfo one seem superior (for various reasons outlined below and with issue 2), it should supersede the other one.

Now here are some ideas/comments from myself that I'm giving for review by the working group:

- about EPP and getting/giving email addresses through poll messages. I think there is a better solution, which the protocol allows today and which is only a matter of policy. It will work only for thick registries, but anyway for thin registries, a solution among registrars will be needed (and I did not have enough time to think about good solutions for thin registries).

So here is the idea: the EPP protocol has a domain:info operation which reveals all data related to the domain, including the contact IDs of the registrant. This operation accept an authInfo code, the idea being that if the registrar doing it is not the current sponsoring registrar of the domain name, it may still get information on it if it has the proper authInfo code (given to him by the admin/registrant which got it from the current sponsoring registrar). At least this is a policy decision, some registries allow domain:info done by all registrars and some do not. But doing so before a transfer, the prospective new registrar can gain information on the registrant (and admin for that matter) contact ID. Now, the contact:info operation works basically the same way (and would thus reveal the associated email address), with an optional authInfo. But small problem here it is not the same authInfo as previously, this later one is attached to the contact, it is like its password (which may or may not have any relation with the password used by clients to manage their domain names through the registrar website). Here comes a small problem, which could be solved in various ways:

* disclosure of the contact authInfo : this may be a problem for contacts handling multiple domain names and if this "password" is used in other areas.

* change of contacts : the domain currently sponsored by registrar A could use contacts created by registrar B. Technical procedures have nothing against that but registries policies may require registrars to only use their own contacts objects.

* changing the authInfo structure for the contact : authInfo is an extensible element, and has been extended already for domain:info (in short, you can give the authInfo related to the domain you query OR you give the authinfo of one of the contact of the domain you query and the ID of this contact, which is called the roid) I think it could be easily extended for contact:info such as you would pass, not the contact authInfo (which would thus remain secret to the future registrar, which is good), but the domain authInfo you wish to transfer and for which the current contact you query is the admin or registrant, and the ID of this contact (which is displayed in the domain:info).

I believe this would need only a minor technical specification (as it has been done for domain:info already), and very little changes in current software both on registrar and registry sides.

So this is only an idea, and maybe further work on it may find it useful or definitively useless. If needed, and useful, I'm available to help study and work around this idea or other ones like that, if my participation could be useful to the working group.

- getting maybe a little too far, but based on the comments I gave previously on authInfo introduction in EPP, the transfer policy could be simplified a lot and at the same time this issue could be resolved if the policy is changed so that it requires *only* the authInfo code to start the transfer, removing the contacts email handling. The current sponsoring registrar would still be allowed to notify contacts and would be allowed to stop the transfer if one of the contacts say so.

The current registrar has all email adresses it needs, and can properly identify the associated contacts and inform them. No emails would need to be passed from registrars to registrars, no technical changes would be required. Things will not go slower than today (as the domain authInfo would still be needed, and so things can be "blocked" if the current sponsoring registrar refuse to give it), they will maybe go a little faster, but more important things will be simpler, without the need of 2 specific acknowledgments needed (authInfo + contacts answer). I do not believe that this simplification creates more risks or ways of disputes.

Even in the very improbable case that this would become the way forward, I would keep my recommendation above to make sure all contacts are handled the same way everywhere.

I specifically do not understand while the report says on page 21 about using only authInfo: "However, this was not deemed a secure and viable solution compared to the current system."

If the authInfo is not secure, why using it at all then ? Why not going back to the previous system, before EPP, with only contacts authorization? If the authInfo is secure, why could it not be secure by itself? In what way do emails, through clear channels (making snooping very easy) and from/to email adresses publicly known in whois (making

---

spoofing/impersonification trivial), make it more secure ? It is not public information (where contacts names emails and so are in whois so open to many kind of attacks... which one specific example even given in the report page 22 about compromised email accounts !), and it is available only to registrars.

This also seem to be the position of the Registry Consistuency as it can be read on page 30.

Again, see my previous discussion about authInfo introduction in EPP.

To summarize, my preferences would be, from most prefered to least:

- first to simplify the policy, to remove the new registrar requirement to send emais to the contacts, and make the transfers mandatory as soon as the authInfo is known, leaving the current sponsoring registrar the possibility to make contacts and refuse the transfer (only if some contacts do explicitely refuse it or for the reasons outlined in the current policy or its march 2009 revision); even if that case, streamlining of the difference between registrant and admin contact should be achieved, and maybe the registrant contact should be taken completely out of the procedure of domain name transfers management.

- if removing this part from the policy is not possible, then I would recommend working on making the registrant contact a same class citizen as the administrative one and maybe taking it out of the equation for the reasons outlined above, and at the same time working either on IRIS and/or EPP (see some ideas above) to see how exchanges of email adresses could be made simpler or exchanged for other authentication, based on the current authInfo.

I'm clearly against any further work on whois as known today to try shoehorning something into it. This energy should be more properly spent on IRIS growth/adoption and/or EPP adjustements. I do note that progressively working on whois replacement in favor of IRIS will have good consequences for transfers (even if only the administrative contact remains concerned, the standardized format of IRIS would make it easier to get access to administrative email address, not even counting about the proper authorization framework

around IRIS access) and other issues, such as display of personal information through current publicly available whois (some issues as being worked on by other working group).

===

Issue 2. About other type of electronic authentications

Like the report says, emails are not always a very good type of authentication. They can be spoofed, hijacked, and redirected (when someones waits for the domain name on which a contact primarily email address is recorded, such as gmail.com in bob@xxxxxxxxx , to be dropped because not renewed - and this has already happened in the past including for very high profiles domain names - and then reregister it and have instant access to all emails directed to it). Which makes me wonder even more about why they are still used as primarily token of authentications during domain name transfers, in contrast of using the more secure authInfo one.

Emails could be protected further by the use of technologies such as OpenPGP and/or S/MIME to ensure integrity, confidentiality and especially authentication (of registrar sending the messages, to prevent phishing, and of the contact replying, to prevent bogus replies). But as far as I know they are not widely used in this case.

Also, access to a website (protected by a SSL certificate), with the browser (and hence the user) authentifying itself with another SSL certificate may be seen as a better security method than current emails.

Many other schemes may be imagined.

I do not think the GNSO/ICANN should start defining these mechanisms through beforehand procedures that would apply uniformly to each registrar.

Registrars should decide if they want to use other methods of authentication, and which ones. It would be a clear and huge factor of differentiation between registrars. Before

starting to use it, they could provide information about their procedure to the relevant registry that would then be notified and could act if it thinks the new mechanism is not good enough. Also (or replacing previous point), yearly ICANN could monitor which mechanisms are used by registrars and verify they meet some requirements, or it can be done during regular registrars auditing and/or when disputes arise for some transfers using some "new" authentication method. Another idea would be to put in place a process similar to the RSTEP one for new registry services.

This would allow the market to invent other means without having to wait for very long procedures beforehand. However some checks after problems or regularly make sure that the whole system is not derailed by some ill attempts. So a correct mixture of free market innovation with some ICANN/GNSO policies to put some boundaries would be my recommendation.

===

Issue 3. Handling partial bulk transfer between registrars

I have no specific ideas on this issue, as it seems something not very frequent. Or at least not very known/heard of.

As I said in my introduction on top, it may help here to have some hard numbers and to know:
- which registries have/had this issue,
- how many registrars does it involve,
- the reasons, if any, for the need of a partial bulk transfer, (specifically because the report speaks about registrar-initiated transfers instead of registrant-initiated, which may mean internal handling of domain names inside a group of registrars controlled by
one and the same entity) ;
- and how many domain names (and/or as percentage of the total portfolio considered for partial bulk transfer)

If these numbers happen to be very low, it may not be a good idea to focalize a lot of resources inside ICANN and the GNSO to think about this issue. Especially because it rise a lot of issues around security, fees, requirements, cases where it can apply or not, etc.

The report gives 5 scenarios (cases) on pages 24 & 25 :
- Partial Bulk Transfer following ICANN accreditation of a reseller I do not believe this happens more than a few times per year. Are there data about that ?
- Partial Bulk Transfer between registrars (end of agreement with one gTLD)
I believe that the registrar concerned knows when it agreement will come to an end (except for failures on this part, but then this is another problem), so it has plenty of time to do transfers before that date.
- Partial Bulk Transfer in case of a (partial) merger or acquisition between registrars
Like first case, I'm not sure this happens a lot per year. Are there data about that ?
- Partial Bulk Transfer initiated by a registrant The report itself previously asserts that this case is already handled directly by registrars as a specific service. Hence no specific new policy may be needed in that case.
- Partial Bulk Transfer following de-accreditation of a registrar SAme case as the first one, and I think it may happen even less frequently. Any data ?

In short I pretty much agree with the report preliminary conclusion, stating that "there is no need to incorporate provisions for handling partial bulk transfers between registrars at this stage"

--
Patrick Mevzek
Dot and Co <http://www.dotandco.com/> <http://www.dotandco.net/>

================================

IRTP-PDP A - Comments from VeriSign

---

* To: <irtp-initial-report@xxxxxxxxx>
* Subject: IRTP-PDP A - Comments from VeriSign
* From: "Steele, Barbara" <BSteele@xxxxxxxxxxxxx>
* Date: Thu, 29 Jan 2009 08:46:58 -0500

Attached, please find VeriSign's response to the request for comments on the Inter Registrar Transfer Policy Part A Policy Development Process Initial Report. Thank you.

Barbara Steele
Compliance Officer / Director of Policy
VeriSign Naming Services

Attachment: 20090129-VeriSign Comments on Initial Report - IRTP PDP A.pdf
Description: 20090129-VeriSign Comments on Initial Report - IRTP PDP A.pdf

VeriSign Comments on the Initial Report on the Inter-Registrar Transfers Policy - Part A Policy Development Process
29 January 2009

Issue 1. Potential need for exchange of registrant email information between registrars
In a poll conducted of the gTLD Registry Operators, it should be noted that the majority of Registry Operators that maintain thick Whois information are contractually required to make the registrant e-mail address available publicly. Further discussion should occur to determine why this is a requirement for some thick Registry Operators but not all and it is not a requirement for any Registrars. Several options for making this information available (ie. modifications to EPP or via IRIS) have been outlined in the report but all would require significant time and expense to implement.

It is our opinion that the suggestion that future IRTP working groups should consider the appropriateness of a policy change that would prevent a registrant from reversing a transfer after it has been completed and authorized by the admin contact should not be put on the

table for discussion as this could make it easier for a domain name to be hi-jacked. Of the transfer dispute cases that have been filed with VeriSign, the second most common ground on which a case is filed is the registrant did not authorize the transfer. (The most common ground is failure by the gaining registrar to provide the Form Of Authorization, or FOA, when requested). If the registrant no longer has the right to dispute a transfer initiated and authorized by the admin contact, it will make it much more difficult for the rightful holder of a domain name to recover a domain resulting in what could be lengthy and expensive court proceedings.

Issue 2. Potential need for including new forms of electronic authentication to verify transfer requests and avoid 'spoofing' VeriSign contends that the AuthInfo code used to further authenticate the transfer of a domain name from one registrar to another appears to have helped in reducing the reported instances of fraudulent inter-registrar transfers. We do not dispute that additional means of electronic authentication may be helpful in further reducing both inter-registrar transfers, as well as internal transfers (or change of registrant). However, VeriSign supports the position that offering such additional security measures should be left up to the registrar to choose whether or not to provide as a part of its offering.

Issue 3. Consider whether the IRTP should include provisions for 'partial bulk transfers' between registrars. At least one Registry Operator and several registrars have implemented solutions / products to address requests for partial bulk transfers between registrars. VeriSign agrees that market solutions should be the preferred method for addressing this issue. Requiring all Registry Operators and registrars to go to the expense to implement a means to effect partial bulk transfers when their customer base may not fit the profile that would benefit from such a solution is not justified when this issue can be adequately addressed via market solutions.
==============

Registrar Constituency Position on Inter-Registrar Transfer Policy Initial Report

   * To: "irtp-initial-report@xxxxxxxxx" <irtp-initial-report@xxxxxxxxx>
   * Subject: Registrar Constituency Position on Inter-Registrar Transfer Policy Initial Report

---

   * From: "Clarke D. Walton" <clarke.walton@xxxxxxxxxxxxxxx>
   * Date: Fri, 30 Jan 2009 17:42:29 -0500

January 30, 2009

Registrar Constituency Position on Inter-Registrar Transfer Policy Initial Report

BACKGROUND

In January 2009, the Registrar Constituency ("RC") was asked to provide feedback regarding the Inter-Registrar Transfer Policy ("IRTP") Initial Report. This Position Paper captures the overall sentiment expressed by the RC Members who provided feedback about this matter. Due to time constraints, however, no formal vote regarding this Position Paper was taken.

RC POSITION

On October 3, 2008 the RC submitted its comments to ICANN regarding the three issues that comprise Part A of the IRTP Policy Development Process. After reviewing the IRTP Initial Report, the RC's current views remain largely the same as they were in October regarding issue 1 and issue 2. Regarding issue 3, however, the RC has revised its view in light of the conclusions reached in the IRTP Initial Report.

 1. Is there a way for registrars to make Registrant E-mail Address data available to one another?

No viable secure implementation of this proposal has been advanced that would enable a policy to require registrars to make Registrant E-mail Address data available to one another.

Additionally, the RC believes that regulatory intervention is not necessary to address this issue. This issue is more appropriate for market based solutions rather than regulatory intervention.

The RC wishes to acknowledge one comment regarding the relationship between the Registrant and Admin Contact. According to the IRTP Initial Report, one question that was brought up during discussion among the Working Group involves a Registrant's authority to overrule the Admin Contact. The RC believes this related sub-issue deserves greater consideration, and the RC plans to examine it during subsequent phases of the IRTP Policy Development Process.

 1. 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).

The RC does not believe that a regulatory approach to authentication is necessary. The RC recommends that the questions of whether additional authentication technology is needed, and if so which technology to implement, be decided based on market demands rather than regulation.

To that end, the RC cautions ICANN about the unintended consequences of technology directives. Specifically, any mandated technology is guaranteed to become the target of hackers who seek to circumvent its security. Having the option of a variety of technologies which may be developed and implemented based on market demands offers greater security in the long-run.

 1. 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.

The RC agrees with the conclusions reached in the Working Group. There is no need to incorporate provisions for handling partial bulk transfers between registrars at this stage. The RC agrees with the Working Group that these scenarios can be addressed either

through the existing Bulk Transfer services offered by some gTLD registries, or through existing market solutions.

 CONCLUSION

The opinions expressed by the RC in this Position Paper should not be interpreted to reflect the individual opinion of any particular RC member.