## RDS PDP WG Poll - 9 May

During our 9 May meeting, the RDS PDP WG continued deliberation on the following charter question:

*What steps should be taken to control “thin data” access?*

This poll gives all WG members an opportunity to confirm, reconsider, or elaborate upon support for possible WG agreements developed during the 9 May meeting. Meeting notes and materials, including a meeting handout to set the stage for deliberating this question, can be found at this link: https://community.icann.org/x/EsPRAw

As a reminder, deliberation is currently focused on "thin data" as defined by the Thick WHOIS Report: "*A thin registry only stores and manages the information associated with the domain name. This set includes data sufficient to identify the sponsoring registrar, status of the registration, creation and expiration dates for each registration, name server data, the last time the record was updated in its Whois data store, and the URL for the registrar’s Whois service.*" This WG previously reached rough consensus that "*Every existing "thin data" element does have at least one legitimate purpose for collection.*" It may be useful to keep these assumptions in mind when responding to this poll.

This poll will close at COB on Saturday 13 May 2017.

*As previously announced, by submitting a response to this poll, you are granting permission for your entire response - including WG member name and response timestamp - to be included in published poll results. Responses submitted by WG members are not assumed to reflect the views of any organization with which they may be affiliated.*

Note: As always, a link to the most recently-opened RDS PDP WG poll, along with links to the last meeting’s notes/recordings and next meeting materials, can be found here: http://tinyurl.com/ng-rds

* 1. **Your name (must be RDS PDP WG Member - not WG Observer - to participate in polls)**

If you are a WG Observer and wish to participate in polls, you must upgrade to WG Member to do so.

2. **Authentication:**
Building on last week's WG agreement: "*gTLD registration "thin data" should be accessible without requiring inquirers to identify themselves or state their purpose*," the WG deliberated this week on whether requestor identification and/or authentication should be disallowed, allowed, or required.

Some WG members expressed concern that authentication not be prohibited by policy – for example, not precluding that a single authenticated query might return the union of "thin data" and additional data elements which the inquirer has permission to access. Other WG members expressed concern that allowing authentication might be misinterpreted as requiring authentication, which was seen as inconsistent with last week's agreement.

To reflect these points of view, the following alternative phrasings for a possible requirement were suggested during and after the WG call. Please indicate your level of support for the alternatives given below, using the "Response" pull-down choices:

- This is my preference
- I could live with this
- I do not support this, or
- Leave blank if no opinion or not applicable.

| | Response |
|---|---|
| a) "Thin data" elements should be accessible with or without requestor authentication. | |
| b) "Thin data" elements should not require requestor authentication, but must allow for optional authentication of the requestor. | |
| c) "Thin data" elements are to be accessible, regardless of the level of authentication of the requestor. | |
| d) "Thin data" elements are to be accessible, regardless of the level of authentication, or lack thereof, of the requestor. | |
| e) "Thin data" elements should be accessible without requester authentication. | |

f) Other (specify)

3. **Operational Controls:**
During further deliberation on possible requirements identified in last week's poll, several WG members suggested splitting deliberation on rate limiting and CAPTCHA from deliberation on access controls.

Some WG members expressed the view that rate limiting and CAPTCHA are merely operational controls (i.e., measures to protect infrastructure from overload or attack), without policy implications. Others expressed the view that policies should explicitly allow for rate limiting and CAPTCHA. To test one possible requirement that may reflect both views, please indicate whether you agree or disagree with the following statement:

*There should be no RDS policies that prevent RDS operators from applying operational controls such as rate limiting and CAPTCHA, provided that they do not unreasonably restrict legitimate access.*

- ◯ Agree
- ◯ Disagree

Comment Box (for example, give rationale for disagreeing):

Thanks for participating in this poll. Please click below to submit your responses.

*By submitting a response to this poll, you are granting permission for your entire response - including WG member name and response timestamp - to be included in published poll results.*

Input gathered through this poll will be used as input to further WG deliberation on charter questions.