Q1 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.

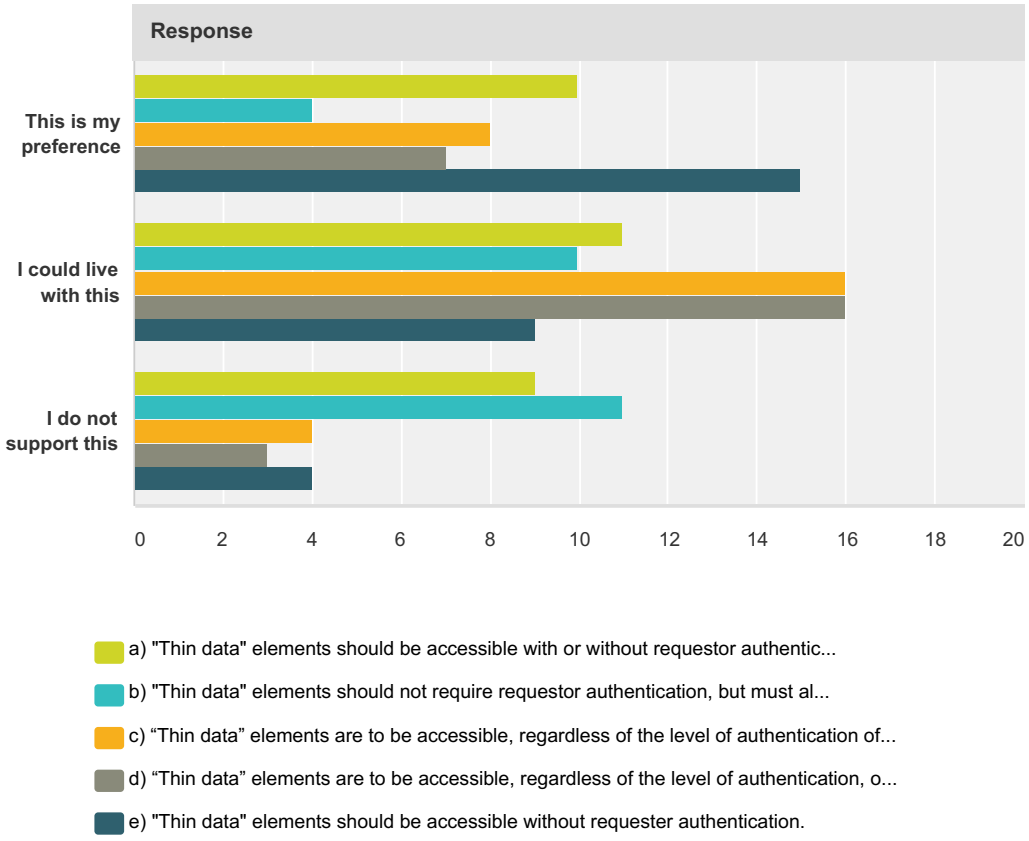
Answered: 33 Skipped: 0

#	Responses	Date
1	Chris Pelling	5/13/2017 12:17 AM
2	Alex Deacon	5/12/2017 7:10 AM
3	Stephanie Perrin	5/12/2017 6:45 AM
4	Fabricio Vayra	5/12/2017 5:36 AM
5	Tom Shaw	5/12/2017 3:24 AM
6	Michael Peddemors	5/12/2017 2:51 AM
7	Benny Samuelsen	5/12/2017 2:48 AM
8	Venkata Atluri	5/12/2017 2:37 AM
9	Susan Prosser	5/12/2017 2:28 AM
10	Allan Liska	5/12/2017 1:20 AM
11	Rod Rasmussen	5/12/2017 1:09 AM
12	Nick Shorey	5/12/2017 12:35 AM
13	Volker Greimann	5/12/2017 12:29 AM
14	Sam Lanfranco	5/12/2017 12:17 AM
15	Klaus Stoll	5/12/2017 12:05 AM
16	Brian Gosch	5/11/2017 1:13 AM
17	MichaelHammer	5/10/2017 5:46 AM
18	allison nixon	5/10/2017 3:05 AM
19	Vicky Sheckler	5/10/2017 2:35 AM
20	Nathalie Coupet	5/10/2017 1:32 AM

21	Adam LLanier	5/10/2017 12:31 AM
22	John Bambenek	5/10/2017 12:22 AM
23	Ayden Ferdeline	5/10/2017 12:03 AM
24	Chuck Gomes	5/9/2017 11:46 PM
25	Patrick Lenihan	5/9/2017 11:28 PM
26	Andrew sullivan	5/9/2017 9:45 PM
27	Natale Maria Bianchi	5/9/2017 9:19 PM
28	Scott Hollenbeck	5/9/2017 9:01 PM
29	Greg Mounier Europol	5/9/2017 6:34 PM
30	Farell Folly	5/9/2017 4:31 PM
31	Sanjeev Gupta	5/9/2017 3:25 PM
32	Greg Aaron	5/9/2017 12:36 PM
33	Kal Feher	5/9/2017 11:16 AM

Q2 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.

Answered: 31 Skipped: 2

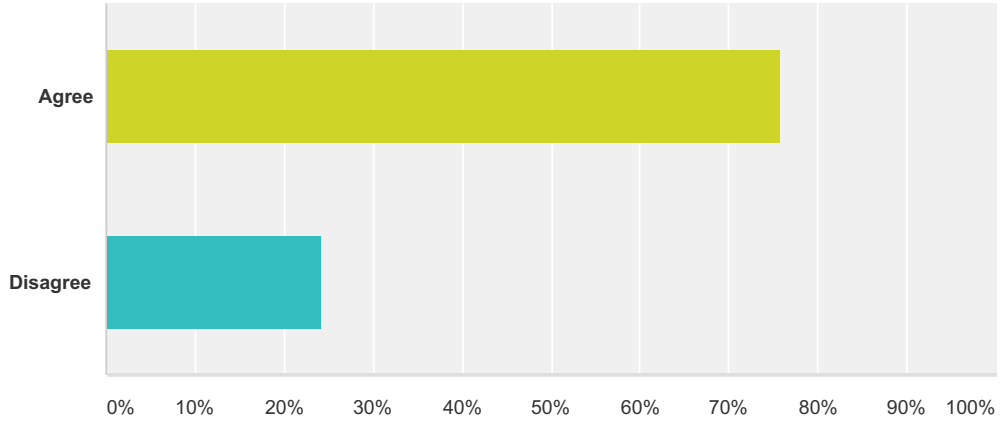


Response						
	a) "Thin data" elements should be accessible with or without requestor authentication.	**b) "Thin data" elements should not require requestor authentication, but must allow for optional authentication of the requestor.**	**c) “Thin data” elements are to be accessible, regardless of the 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.**	**Total**
This is my preference	**22.73%** 10	**9.09%** 4	**18.18%** 8	**15.91%** 7	**34.09%** 15	44
I could live with this	**17.74%** 11	**16.13%** 10	**25.81%** 16	**25.81%** 16	**14.52%** 9	62
I do not support this	**29.03%** 9	**35.48%** 11	**12.90%** 4	**9.68%** 3	**12.90%** 4	31

#	f) Other (specify)	Date
1	Requestors must have access to thin data elements without either identifying or authenticating themselves. It is recognized that some data elements currently forming part of the thin data set may be removed upon further deliberations on data elements.	5/12/2017 6:45 AM
2	"Thin data" elements are to be accessible without requester authentication.	5/12/2017 2:28 AM
3	only with requestor authentication	5/12/2017 12:05 AM
4	If "b" is intended to convey authentication in conjunction with thick data then I could live with it.	5/10/2017 5:46 AM
5	"Thin data" elements must be accessible without authentication.	5/10/2017 12:31 AM
6	Requestors must have access to thin data elements without either identifying or authenticating themselves. It is recognized that some data elements currently forming part of the thin data set may be removed upon further deliberations on data elements.	5/10/2017 12:03 AM
7	I think that Greg Aaron and Stephanie Perrin made some good comments about this poll on the WG list and think we should continue to refine the wording of any conclusions we consider in our meeting next week.	5/9/2017 11:46 PM
8	I still insist that requestor needs to indicate the purpose..This is vital later when resolving spamming ussues resulting from that data. For a law application, it is important to know that users specify different purpose than the one they actually use the data for.	5/9/2017 4:31 PM
9	Access to thin registration data must be provided to anonymous requestors, without any type of authentication.	5/9/2017 12:36 PM
10	Note that options C,D use the word 'authentication' in a manner that 'authorisation' is typically used.	5/9/2017 11:16 AM

Q3 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.

Answered: 33 Skipped: 0



Answer Choices	Responses	
Agree	**75.76%**	25
Disagree	**24.24%**	8
Total		**33**

#	Comment Box (for example, give rationale for disagreeing):	Date
1	My agreement is only given as long as no "automated" or "automation" tools are used.	5/13/2017 12:17 AM
2	Operators must be able to block bulk access.	5/12/2017 6:45 AM
3	Captcha impeeds integration with systems like MISP and othe data enroichment systems. I would suggest API Keys instead.	5/12/2017 3:24 AM
4	I agree on controls such as rate limiting, I do not agree on CAPTCHA	5/12/2017 2:51 AM
5	I agree with the sentiment of the statement, but I feel it is poorly worded, it is never a good idea to use a double negative. I feel a better wording would be something along the lines of "RDS operators should be allowed to apply reasonable operational controls..."	5/12/2017 1:20 AM
6	Given the current state of play, where registrars use operational controls to game the system on access, I believe policy needs to be more explicit than "unreasonably restrict" as the definition of "reasonable" may vary widely. In general I support the concept, but past bad behavior requires better vigilence in new policy.	5/12/2017 1:09 AM
7	The language in this statement (such as; unreasonably; legitimate) is too vague and ambiguous.	5/12/2017 12:35 AM
8	RDS should be protected by such operational controls to prevent data harvesting and bulk inquiries.	5/12/2017 12:29 AM
9	With the proviso that there should be additional requirements for minimum acceptable rates (per user/IP Address and perhaps global minimum capacity.	5/10/2017 5:46 AM
10	too often in other contexts, we see these controls used precisely to restrict legitimate access	5/10/2017 2:35 AM
11	CAPTCHA will restrict bulk machine queries (see Allison Nixon's argument)	5/10/2017 1:32 AM

12	Whatever language allows for unauthenticated access to thin data and still allows for relevant controls to prevent abuse (capcha / rate-limiting / etc)	5/10/2017 12:22 AM
13	RDS operators should be free to implement rate limiting and CAPTCHAs if they wish to do so. The precise number of queries I will lead to them to decide. However I am thinking that no user should be able to perform more than 1,000 queries per day.	5/10/2017 12:03 AM
14	The condition that rate limiting and CAPTCHA 'not unrreasonably restrict legitimate access' is a critical element in my opinion, one that was explained by several people on the WG call.	5/9/2017 11:46 PM
15	Of course, this entails that we define "reasonable" and "legitimate" for these purposes	5/9/2017 9:45 PM
16	What is "reasonable" and "unreasonable" ? Some organizations in the security field have a real need for massive volumes of queries, just a consequence of massive abuse. Being rate limited becomes indistinguishable from being denied access, so the issues are quite intertwined and should be treated within a single policy umbrella. Authentication can allow per-user thresholds, and I support authentication primarily for being able to be granted high query volumes for my organization.	5/9/2017 9:19 PM
17	The above language contains loopholes. There should be policies about rate limiting, namely what reasonable and unreasonable restrictions may consist of.	5/9/2017 12:36 PM