

Michelle DeSmyter:Dear all, Welcome to the GNSO Next-Gen RDS PDP Working Group call on Tuesday 09 May 2017 at 16:00 UTC.

Michelle DeSmyter:Meeting agenda page:

https://urldefense.proofpoint.com/v2/url?u=https-3A_community.icann.org_x_EsPRAW&d=DwIFaQ&c=FmY1u3PJp6wrcrw113mSVzgfkbPSS6sJms7xcl4I5cM&r=8_WhWIPqsLT6TmF1Zmyci866vcPSF04VShFqESGe_5iHWG1BLwwehFBfjrsjWv9&m=1QvZPa0jqhCG5cB2idF0ww4YIt20ReibUHXLKJymI34&s=m5BDCwOsnoXbuUY5nyWPqgN7jyUjwZTa3Xh98YGERKE&e=

Chuck Gomes:Hello all

Lisa Phifer:RDS PDP WG Newcomers, if you may be interested in a one-hour tutorial, please complete this survey:

https://urldefense.proofpoint.com/v2/url?u=https-3A_www.surveymonkey.com_r_3GG6CRR&d=DwIFaQ&c=FmY1u3PJp6wrcrw113mSVzgfkbPSS6sJms7xcl4I5cM&r=8_WhWIPqsLT6TmF1Zmyci866vcPSF04VShFqESGe_5iHWG1BLwwehFBfjrsjWv9&m=1QvZPa0jqhCG5cB2idF0ww4YIt20ReibUHXLKJymI34&s=NxVZzqFhoi2iNXgmAMwAg2eIhRilRPcHqfmikoFODPo&e=

Fabricio Vayra:hello, all!

Venkata Atluri:Hello Everyone

Maxim Alzoba (FAITID):Hello All

Maxim Alzoba (FAITID):I will have to drop after 60 minutes

Michael Hammer:Greetings

Chuck Gomes:How's the GDD Summit Maxim?

Maxim Alzoba (FAITID):good so far

Lisa Phifer:Displayed on-screen:

https://urldefense.proofpoint.com/v2/url?u=https-3A_community.icann.org_download_attachments_64078610_AnnotatedResultsV2-2DPoll-2Don-2DPurpose-2Dfrom-2D2MayCall.pdf&d=DwIFaQ&c=FmY1u3PJp6wrcrw113mSVzgfkbPSS6sJms7xcl4I5cM&r=8_WhWIPqsLT6TmF1Zmyci866vcPSF04VShFqESGe_5iHWG1BLwwehFBfjrsjWv9&m=1QvZPa0jqhCG5cB2idF0ww4YIt20ReibUHXLKJymI34&s=uxzZv_WYEA_CCDWawcFd0yygM8IQyAkLYf3SSYkxzBno&e=

Michelle DeSmyter:Remmy

Lisa Phifer:Q2 results are on page 3

Lisa Phifer:WG Agreement to be recorded in our deliberation working draft: gTLD registration "thin data" should be accessible without requiring inquirers to identify themselves or state their purpose.

Marika Konings:Please note that the charter outlines the process for determining consensus and level of consensus.

Lisa Phifer:All points of rough consensus are captured in our working document; the latest draft is

https://urldefense.proofpoint.com/v2/url?u=https-3A_community.icann.org_download_attachments_56986791_KeyConceptsDeliberation-2DWorkingDraft-2D21April2017.pdf&d=DwIFaQ&c=FmY1u3PJp6wrcrw113mSVzgfkbPSS6sJms7xcl4I5cM&r=8_WhWIPqsLT6TmF1Zmyci866vcPSF04VShFqESGe_5iHWG1BLwwehF

[BfjrsjWv9&m=1QvZPa0jqhCG5cB2idF0ww4YIt20ReibUHXLKJymI34&s=d3L9zG4ZV6dKQ9-xxsdLhIP4o_fjo1gh7cFpyqLWUm8&e=](https://urldefense.proofpoint.com/v2/url?u=https-3A_community.icann.org_display_gTLDRDS_Phase-2B1-2BDocuments&d=DwIFaQ&c=FmY1u3PJp6wrcrwl13mSVzgfkbPSS6sJms7xc14I5cM&r=8_WhWIPqsLT6TmF1Zmyci866vcPSF04VShFqESGe_5iHWG1BLwwwhFBfjrsjWv9&m=1QvZPa0jqhCG5cB2idF0ww4YIt20ReibUHXLKJymI34&s=d3L9zG4ZV6dKQ9-xxsdLhIP4o_fjo1gh7cFpyqLWUm8&e=)

Lisa Phifer:The most recent version of our working document is always posted at the top of this wiki page:

https://urldefense.proofpoint.com/v2/url?u=https-3A_community.icann.org_display_gTLDRDS_Phase-2B1-2BDocuments&d=DwIFaQ&c=FmY1u3PJp6wrcrwl13mSVzgfkbPSS6sJms7xc14I5cM&r=8_WhWIPqsLT6TmF1Zmyci866vcPSF04VShFqESGe_5iHWG1BLwwwhFBfjrsjWv9&m=1QvZPa0jqhCG5cB2idF0ww4YIt20ReibUHXLKJymI34&s=y3BdD9LZAUMiQNbxybTHxTP2v0NCVw43dbEGec1qv0o&e=

Lisa Phifer:Agreements on data element requirements (thin and otherwise) will also be recorded in that working draft, under the Data Elements charter question

Lisa Phifer:Q3 results start on page 5

Lisa Phifer:We will be displaying this handout for further deliberation momentarily:

https://urldefense.proofpoint.com/v2/url?u=https-3A_community.icann.org_download_attachments_64078610_Charter-2520Question-25205-2520-2D-2520Handout-2520-2D-2520For9MayCall.pdf&d=DwIFaQ&c=FmY1u3PJp6wrcrwl13mSVzgfkbPSS6sJms7xc14I5cM&r=8_WhWIPqsLT6TmF1Zmyci866vcPSF04VShFqESGe_5iHWG1BLwwwhFBfjrsjWv9&m=1QvZPa0jqhCG5cB2idF0ww4YIt20ReibUHXLKJymI34&s=QVV8-1EIFOLrguivnaSSqAftjK81HmBa2VpZ8MvcxQ&e=

andrew sullivan:Apparently I am incompetent and failed somehow to save my answers, but in any case, I have no idea how (2) is supposed to work

Lisa Phifer:What we conclude from Q3 is that there is interest in deliberating these - this poll question did not seek agreement or disagreement to each possible requirement

Lisa Phifer:Displayed on-screen:

https://urldefense.proofpoint.com/v2/url?u=https-3A_community.icann.org_download_attachments_64078610_AnnotatedResultsV2-2DPoll-2Don-2DPurpose-2Dfrom-2D2MayCall.pdf&d=DwIFaQ&c=FmY1u3PJp6wrcrwl13mSVzgfkbPSS6sJms7xc14I5cM&r=8_WhWIPqsLT6TmF1Zmyci866vcPSF04VShFqESGe_5iHWG1BLwwwhFBfjrsjWv9&m=1QvZPa0jqhCG5cB2idF0ww4YIt20ReibUHXLKJymI34&s=uxzZv_WYEA CCDWawcFd0yygM8IQyAkLYf3SSYkxzBno&e=

andrew sullivan:I sort of feel like a number of people imagine all access to this data is by a human looking at it

Rod Rasmussen:@Andrew - by (2) did you mean 3b?

andrew sullivan:yes, 3b

Lisa Phifer:If you wish to be able to refer offline to your own comments, once we move on to deliberation

Rod Rasmussen:See my comment - what's even the point?

andrew sullivan:Indeed

Lisa Phifer:Handout now displayed on-screen:

https://urldefense.proofpoint.com/v2/url?u=https-3A_community.icann.org_download_attachments_64078610_Charter-2520Question-25205-2520-2D-2520Handout-2520-2D-2520For9MayCall.pdf&d=DwIFaQ&c=FmY1u3PJP6wrcrwl13mSVzgfkbPSS6sJms7xcl4I5cM&r=8_WhWIPqsLT6TmF1Zmyci866vcPSF04VShFqESGe_5iHWG1BLwwwehFBfjrsjWv9&m=1QvZPa0jqhCG5cB2idF0ww4YIt20ReibUHXLKJymI34&s=QVV8-1EIFOLrguivnaSSqAftjK81HmBa2VpZ8MvcxQ&e=

Lisa Phifer:Page 2 gives WG Agreement from last week as foundation for further deliberation on possible requirements for controlling access to "thin data"

Lisa Phifer:Page 3 uses results from poll question 3 to just lay out several different possible requirements for deliberation in this call

Alan Greenberg:Sorry to be late.

Lisa Phifer:Current RAA WHOIS specification allows rate limiting

Lisa Phifer:someone has an open mic

Rod Rasmussen:3rd item may have a technical aspect but is driven by policy.

Michael Hammer:+1 to Rod's comment.

Lisa Phifer:@Rod, mute your speakers when talking

Marika Konings:Jim, it looks like your microphone is still open

Greg Shatan:Someone needs to mute or be muted.

Michael Hammer:For example, rate limiting to a very low rate might be used to drive people to a pay offering - that is policy, not technical.

Rod Rasmussen:Not my speakers.

Amr Elsadr:@Rod: We're on slide 3 now.

Lisa Phifer:We are discussing possible requirements on page 3 of displayed document

Alan Greenberg:Please, WHISH SLIDE?? We all have scrolling

Greg Aaron:So for the purposes of the current discussion, are we talking about thin data only?

Rod Rasmussen:Thanks - explains the disconnect

Lisa Phifer:Yes, we are deliberating "What steps should be taken to control thin data access" - thin data only

Lisa Phifer:@Scott, when querying a gTLD domain name to retrieve "Thin Data" elements... might be better?

andrew sullivan:Friendly amendment, then: "_Requestor identification_ for access to thin data elements should be..." and so on

Lisa Phifer:@Andrew, for example: 1) Requestor identification for access to "thin data" elements should be a) Disallowed, b) Allowed but not required, or c) Required

Scott Hollenbeck (Verisign):@Lisa: maybe, if we assume that people explicitly submit queries for access to subsets of the

available data

Vicky Sheckler:apologies but I've been called away unexpectedly

Vicky Sheckler:will catch up later

Greg Aaron:No, Stephanie, you are not correct.

Lisa Phifer:@Scott, if there are multiple requirements that apply to a particular scenario, they must all be taken into account, but for right now we focus on requirements for any scenario that involves access to "thin data"

andrew sullivan:@Lisa, Scott: I think the point is that if you put it in terms of "elements" then the response to an unauthenticated (or whatever) query isn't allowed to get non-thin data

Scott Hollenbeck (Verisign):@Andrew: yes

andrew sullivan:I agree that the phrasing is a little infelicitous, in that it suggests that people query for particular data

andrew sullivan:I don't think I understood Rod's point about multiple interfaces

andrew sullivan:it seems to me that if we have an RDAP system, and unauthenticated access is permitted to some subset of data, then if you send a query without authentication you get the small subset

andrew sullivan:and if you send a query while authenticated you get the answer you're supposed to

Scott Hollenbeck (Verisign):@Lisa: then I think we should be discussing the conditions under which you have access to only thin data

steve metalitz:Isn't the status quo on #1 and 2 (a) (disallowed); and if so, what would be gained by moving to (b) (requestor ID required or some form of authentication required in some cases but not others)?

Lisa Phifer:@Andrew, what you describe is what the EWG recommended - with the exception that authentication was not the only criteria applied to determine what data elements you are authorized to receive in your reply

andrew sullivan:no, the status quo on all of it is completely unauthenticated and unidentified permission.

andrew sullivan:@Lisa: I know

Scott Hollenbeck (Verisign):@steve: access control decisions can be made if the server knows something about the client asking the question.

Greg Shatan:The Velvet Hammer.

Michael Hammer:Apologies, dropped audio connection

Lisa Phifer:@Scott, Andrew - How in WHOIS today can a requestor identify or authenticate themselves?

Scott Hollenbeck (Verisign):@Lisa: no can do

andrew sullivan:@Lisa some registries at some point ran a VPN with authentication to connect and a whois behind it

Scott Hollenbeck (Verisign):(except for web-nased interfaces that accept server-assigned user names and passwords)

andrew sullivan:but that's pretty weak broth

Lisa Phifer:@Michael - not requiring identification is different than disallowing identification, thus we are probing further with 1)

Rod Rasmussen:My point on different "interfaces" can also be thought of as needing to make different types of queries depending upon the type of request you're making. I would argue that you should get "thin" data for "free" when you're making a gated data element(s) query. If you you have to make two different queries

steve metalitz:@Greg, isn;t another way of saying that that 1 and 2 should be answered (a)?

Rod Rasmussen:My point on different "interfaces" can also be thought of as needing to make different types of queries depending upon the type of request you're making. I would argue that you should get "thin" data for "free" when you're making a gated data element(s) query. If you "disallow" requestor identification for thin data, then you have to make two different queries to get the data you need - one with your ID and one without.

Lisa Phifer:From a policy perspective, rate limiting and CAPTCHA can be allowed or required as anti-abuse measures - or they can be allowed purely to meet operational needs. The latter is the situation in today's WHOIS?

Greg Aaron:Yes, Steve; in order for us to be consistent with ourselves then 1 and 2 should be answered (a).

Lisa Phifer:@Greg, for 1 and 2, how is b) Allowed but not required, inconsistent with last week's agreement?

Maxim Alzoba (FAITID):We should not forget that real infrastructure (CPUs, Memory, storage) add costs , so the issue is to make real "bandwidth" balanced (there is no such thing as truly limitless perfomance)

Rod Rasmussen:OK, we have a wording issue here that's creating a bit of a problem in 1 & 2 - disallowed for *only* thin access but *allowed* when you're making a more complex query to catch my concern.

Lisa Phifer:@Rod, +1

Maxim Alzoba (FAITID):need to drop the call, bye all

Greg Aaron:Lisa: are you saying 'give the requestor the option of identifying himdelf/herself?' But in all cases, give the thin data to requestors whether ort not they have identified themselves?

andrew sullivan:have to step away for a moment

Lisa Phifer:Suggest that we try to derive possible statements from 1/2, separately from 3/4, to describe what policy requirements may apply to thin data access

Rod Rasmussen:That's the gist of it @Greg

Lisa Phifer:@Greg, yes

Greg Shatan:Agree, thick data should "embrace" thin data.

Greg Shatan:in terms of a query response.

Lisa Phifer:@Rod, Requestor Authentication should be allowed but not required for access to any data elements (including thin data elements)?

Daniel K. Nanghaka:I think Requester Identification should be allowed because it helps in enhancement the legitimacy of the Requester

Lisa Phifer:Actually that's probably not it... but is that going in the direction you meant?

Greg Aaron:So my questions are 1) doesn't that create inefficiencies as Rod says, 2) if you collect requestor info then do those people a right to opt out and remove their info from the database later, 3) are registries going to sell data about who queries WHOIS? ICANN might need policy around that....

andrew sullivan:back

Daniel K. Nanghaka:@Greg, then they should have the consent to to opt out - but if you are going to query the data again then I do not see the reason to remove your info from the database

Michael Hammer:If the answer to #1 is a) then question #2 becomes meaningless.

Lisa Phifer:Would it be helpful to divvy deliberation on access methods: web, bulk, protocol queries - and look at access requirements for each?

Daniel K. Nanghaka:And yes, ICANN will need a policy towards user data and authentication of the Requester

andrew sullivan:I think it is obvious that if someone gets a superset of thin data by authentication, then it is ok that they get the thin data along with it

andrew sullivan:but I do not want a registr[y|ar] to be able to decide unilaterally to require authentication

Lisa Phifer:@Andrew, not if authentication is disallowed by policy

andrew sullivan:@Lisa: that's the reason that Scott's worried about how this is phrased

andrew sullivan:because you get that effect if only because of how it's phrased

Rod Rasmussen:@Andrew - yep, it's obvious, so that's why I'm sayin' it - too many times I've seen "obvious" missed in creation of policy. :-)

andrew sullivan:@Rod: oh yes, strongly agree

Lisa Phifer:@Andrew, can you suggest a possible requirement that allows authentication but does not require authentication for access to thin data elements?

Michelle DeSmyter:one moment

andrew sullivan:The point is that an unauthenticated requestor MUST have access to thin data elements, within the required operational bounds of the service (so rate limiting for anti-DoS is acceptable)

andrew sullivan:But authenticated users might have access to other data elements

steve metalitz:Could this be resolved by changing the beginning of each statement to "To the extent querying gTLD 'thin data' elements only,"?

Greg Aaron:+1 Andrew

Fabricio Vayra:+1 Andrew

Scott Hollenbeck (Verisign):@Andrew! YES!

Lisa Phifer:This is why EWG differentiated between the minimum public data set and gated data elements. Public data is accessible with or without authentication. Gated data requires authentication.

Lisa Phifer:Possible requirement: "Thin data" elements must be accessible with or without authentication.

andrew sullivan:Not a complication, but not part of this protocol. As Scott has already pointed out, you get those permissions out of band using your authentication and authorization mechanism

Lisa Phifer:This would be in addition to last week's agreement: "Thin data" should be accessible without requiring inquirers to identify themselves or state their purpose.

Lisa Phifer:Possible requirement: "Thin data" elements must be accessible with or without authentication.

andrew sullivan>Last week's agreement was for "accessibility". It didn't say that was the only way thin elements were accessible

steve metalitz:@Lisa that would change the answer to 2 to (b). Still don't understand rationale for that

Lisa Phifer:@Steve, it allows a single authenticated query to return both thin and thick data elements

Greg Aaron:"Thin data"elements must be accessible with or without authentication" can be interpreted TWO differnt ways, and one of those ways is not what we want.

andrew sullivan:@Greg: what's the second way?

Greg Shatan:My concern is that it can be read to allow authentication to be required when only thin data elements are being requested.

Greg Shatan:I'm the other Greg but that's my thought on the second way.

steve metalitz:"Thin data elements must be accessible with authenticatoin" implies that that they need not be accessible without authentication.

Greg Shatan:Lawyers are never evil, they are only carrying out the desires of clients, who may be evil.

Stephanie Perrin:We use a disjunctive comma to imply the second interpretation, do we not?

Lisa Phifer:Possible alternative: "Thin data" elements must not require authentication, but must allow for optional authentication of the inquirer

andrew sullivan:@Stephanie: this is what happens when people don't follow Oxford on commas :-D

steve metalitz:@Lisa we are getting way ahead of ourselves to torture this lanaguage to accommodate a gated access structure for "non-thin" data which we have not even begun to discuss.

Stephanie Perrin:I know, so much confusion when you forget the importance of commas.....

Lisa Phifer:@Steve, we are trying to be clear that we are not precluding authentication by policy

Daniel K. Nanghaka:Accessibility is open and authentication can be be an option with multiple access of the data

andrew sullivan:@Lisa: how about Thin data elements are to be accessble regardless of the level of authentication of the requestor?

Greg Aaron:Agree with Greg S.

steve metalitz:+1 to Andrew's last formulation.

Lisa Phifer:@Andrew, I think that works

steve metalitz:my coments are in chat, thanks. .

Lisa Phifer:Possible alternative (from Andrew): Thin data elements are to be accessble regardless of the level of authentication of the requestor

Michael Hammer:how about Thin data elements are to be accessble regardless of the level of authentication, or lack thereof, of the requestor?

Nathalie Coupet:@Chuck: Question: What would consumers need to do to be able to identify the author of a website besides going to court and getting an injunction?

Nathalie Coupet:Question

Stephanie Perrin:The simpler the better.

Nathalie Coupet:From thin data

Greg Shatan:The question of how and whether our policies cover third-partying data stores of RDS information (e.g., a service provider).

Greg Aaron:Have we defined "authentication"? The dictionary

defines authentication as: "the process or action of proving or showing something to be true, genuine, or valid." So if you require a requestor's email address, that is not authentication. And under the language being discussed, registries[rars) could request all kinds of info, such as email addresses.

Daniel K. Nanghaka: I think the levels of Authentication are needed

Greg Shatan: I don't have a problem with the concept that Lisa just stated.

Daniel K. Nanghaka: because if the data is beyond thin data then there is a need for authentication

Greg Shatan: It's just the "doctrine of unintended consequences" at play here in the current formulation.

Greg Shatan: Daniel, we are just discussing thin data at the moment.

Michael Hammer: need? or desire for authentication?

Lisa Phifer: @Daniel, if the WG should agree that authentication is allowed or required, then it would define level(s) of authentication. But if authentication is disallowed, there are no levels to define.

andrew sullivan: @Greg A: if the server operator asks for an email address but doesn't check that it works, then it's not authentication. If there is an email-send-use-this-URL loop, then it's weak authentication

Nick Shorey: re ccTLDs - if sharing with ccNSO just bear in mind that not all ccTLDs are members of ccNSO

andrew sullivan: For whatever it's worth, I think I'm on the record in favour of the Data of Record approach

Lisa Phifer: Newcomer tutorial survey:

https://urldefense.proofpoint.com/v2/url?u=https-3A_www.surveymonkey.com_r_3GG6CRR&d=DwIFaQ&c=FmY1u3PJp6wrcrw113mSVzgfkbPSS6sJms7xcl4I5cM&r=8_WhWIPqsLT6TmF1Zmyci866vcPSF04VShFqESGe_5iHWGlBLwwehFBfjrsjWv9&m=1QvZPa0jqhCG5cB2idf0ww4YIt20ReibUHXLKJymI34&s=NxVZzqFhoi2iNXgmAMwAg2eIhRilRPcHqfmikoFODPo&e=

Venkata Atluri: Thank you all

andrew sullivan: bye all

Nathalie Coupet: Bye

Daniel K. Nanghaka: bye all

Nick Shorey: Ciao