

Annotated Results from 6 June RDS PDP WG Poll

**Q2. Expiration Date**

In our 6 June call, the WG considered whether any of the "thin data" elements shown in the example WHOIS record above are NOT required as "thin data" to be made publicly accessible through an RDS. During that discussion, the following agreement was proposed: **Expiration Date should be removed as a "thin data" element accessible without authentication through an RDS.** To help the WG make progress on this question, please indicate whether you agree with this proposal.

Q2	Remove Expiration Date? 9 Agree, 19 Disagree, 3 Unsure Comments from those who disagreed or were unsure
Tim Chen	the Expiration Date is useful for classifying domains as not malicious
Susan Kawaguchi	Expiration data is critical for ruling out issues with a domain names and does not provide PII.
Steve Metalitz	I support the arguments provided by WG members for why the status quo of unauthenticated access to this data element should be preserved.
Rod Rasmussen	This is an operational element for many large-scale processes - unconvinced by arguments that it presents a privacy concern
Andrew Sullivan	I posted an argument about this to the list. It is important for troubleshooting in a distributed network.
Maxim Alzoba (unsure)	since all current systems pull the data from the THIN Registry, such change will cause unnecessary requests to Registrars WHOIS servers in each of the occasions of such requests.
Greg Shatan	The rationale offered for making expiration date inaccessible was not remotely convincing. (I find it odd that those who answer agree are not asked to provide a rationale!) Expiration Date is an important factor for a variety of uses, e.g., based on my experience, due diligence, domain name management, audits, etc.
Michael Haffely	Registration dates can be used to find "new" domains and bad actors creating domains for hosting purposes
Greg Aaron	Expiration Date is essential for renewal and transfer operations, among other things. And there is absolutely no reason, privacy or otherwise, to withhold publication of this field.
Michael Peddemors	Used In automated data analytics, and to automate warnings to the postmaster of domains who host email on our platforms before email interruption occurs due to expiry
John Bambenek	This is important operational and diagnostic info and if contact info is not in RDS, this information is absolutely non-weaponizable (who do you spam if there is no contact info). It is important for machine learning, automated security analysis, and anti-abuse efforts.
Adam Lanier (unsure)	Expiration date is a valuable data element and is useful for troubleshooting and analysis
Vicky Sheckler	Andrew Sullivan's comments to the list explain why expiration date should be included
Michael Hammer	The proposal to remove Expiration Date as a "thin data" element was based on the assertion that it is personal data. It is no more thin data than other elements and is commonly used for a variety of legitimate purposes.
Sam Lanfranco	Creation and expiry dates have legitimate uses. Long long registrations mean being expose to renewal/expiry date abuse is infrequent. Other approaches to curb it should be explored
jonathan matkowsky	There is no rational basis to remove this critical element

**Q3. DNSSEC**

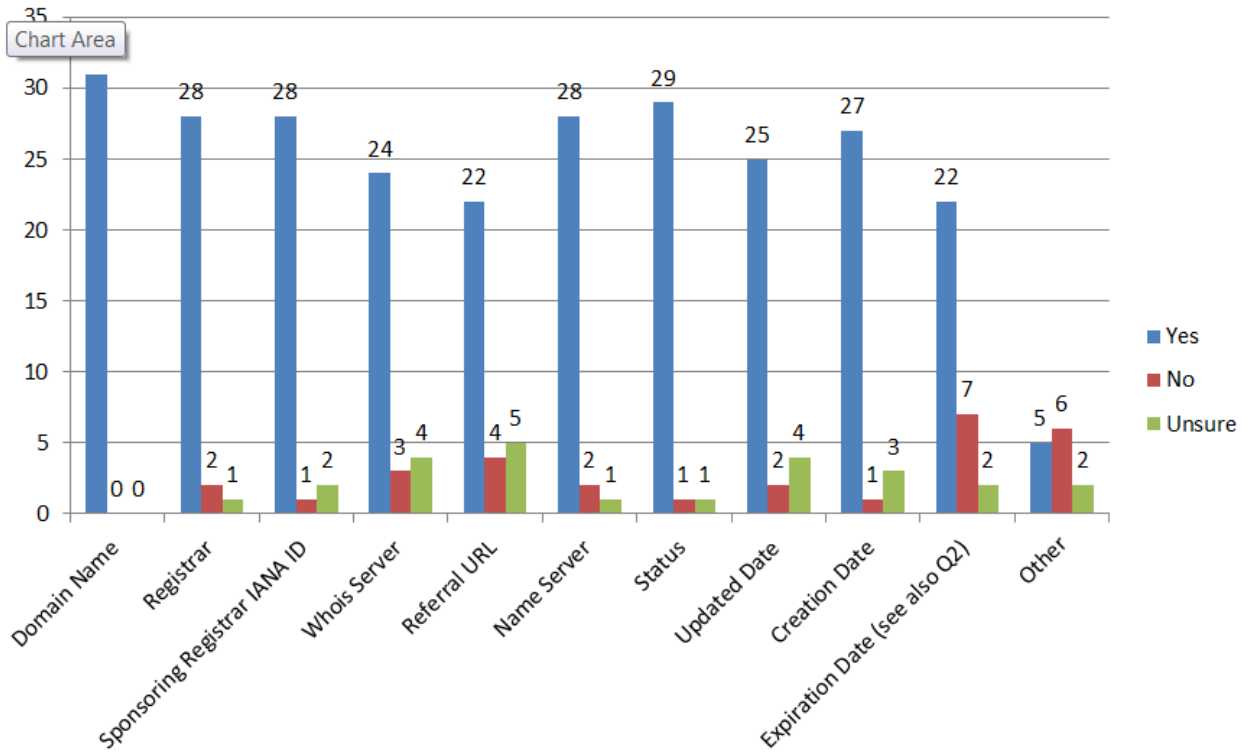
In our 6 June call, the WG considered whether there might be any NEW elements required as "thin data" elements to be made publicly accessible through an RDS. During that discussion, the following agreement was proposed: **DNSSEC should be added as a "thin data" element accessible without authentication through an RDS.** Note: This data element was added in the 2013 RAA; for example, **DNSSEC: signedDelegation** or **DNSSEC: unsigned**. To help the WG make progress on this question, please indicate whether you agree with this proposal.

Q3	Add DNSSEC? 26 Agree, 0 Disagree, 5 Unsure Comments from those who were unsure
<b>Stephanie Perrin</b>	I am really uncertain about what this data element is used for, whether its release could in any way negatively affect an individual etc. I expect it would be fine, but I don't know enough to say for sure.
<b>Ayden Férdeline</b>	I do not have enough knowledge of what DNSSEC is, or why it should be added to the thin data elements, to make such an assessment.
<b>Rob Golding</b>	DNS info, Nameserver info etc is already available through the correct systems, and should not be added to "bloat" and confuse via whois/rds
<b>Michele Neylon</b>	I don't feel strongly either way but happy to see it added
<b>Volker Greimann</b>	It has not been needed until now, so adding it would require some justification beyond it being nice to have.

**Q4. Sufficient "Thin Data" elements**

In our 6 June call, the WG considered the question: **Are today's gTLD WHOIS registration data elements classified as "thin" sufficient at this time?** Some WG members questioned whether all existing data elements (notably statuses and dates) are necessary in "thin data." Other WG members provided examples to illustrate why certain elements are needed in "thin data."

To help the WG make further progress on this question, please indicate whether or not you believe each of the following elements must be included in "thin data" made publicly accessible through an RDS.



Annotated Results from 6 June RDS PDP WG Poll

Q4 All comments provided (color reflects "Other" response: No/Unsure/Yes)	
<b>Ayden Férdeline</b>	We should keep information which is publicly available to the minimum, which is the domain name itself, the name servers, and its status (registered/unregistered). All other information is registrar-registrant contract information.
<b>Tim Chen</b>	Reseller. a proxy for Registrar, which is already in Thin Whois. Potentially useful for classifying domains as malicious.
<b>Steve Metalitz</b>	First, I agree with those who have stated that it is somewhat misleading to equate the label of "thin data" with the characteristic of "unauthenticated public access." "Thin data" has a specific meaning in the context of the "thin" and "thick" Whois models and that definitional difference was never intended to imply any specific difference in the characteristics of public access to the data elements falling on either side of the definitional divide. Second, it is inappropriate to use this exercise to demand that WG members provide an exhaustive list of data elements that should be publicly accessible without authentication, which is what this question seems to be asking. Instead the WG should be looking at each existing data element now included via Whois, and any other data elements proposed, and deciding on a recommendation regarding the modalities of public access to that element.
<b>Rob Golding</b>	status, expiry date etc provide additional abuse vectors and are not necessary for the "public" to know, only the registrar/registrant
<b>Rod Rasmussen</b>	Reseller if applicable - in a reseller model, the reseller is actually more important than the registrar in many use cases that would otherwise involve the registrar.
<b>Andrew Sullivan</b>	DNSSEC stuff, as above. Also, registrar and IANA ID are strictly redundant and in RDAP are not both needed. The whois server can be ditched if whois is ditched. The referral URL becomes more complicated under RDAP and is needed for the functioning of the system.
<b>Paul keating</b>	Any data that does not specifically identify an individual registrant and is relevant to the ownership of the domain
<b>Volker Greimann</b>	Whois Server: This would be replaced by RDS entirely, so there would be no more need.
<b>Greg Aaron</b>	These fields are also included in thin data as per the 2013 RAA and the new gTLD Base Agreement: DNSSEC data, Registrar IANA ID, Registrar Abuse Contact Email, Registrar Abuse Contact Phone, Reseller [reseller field optional for registrar to populate].
<b>Sam Lanfranco</b>	Not sure of legitimate needs for Updated Date, or benefits of deletion.
<b>jonathan matkowsky</b>	Registrar abuse contact; reseller name and contact URL

All results shown here were extracted from:

- SurveyMonkey Summary Poll Results: [SummaryResults-Poll-from-6JuneCall.pdf](#)
- SurveyMonkey Raw Data Poll Results: [RawDataResults-Poll-from-6JuneCall.zip](#) and [XLS](#)