Draft Framework for a Possible Unified Access Model for Continued Access to Full WHOIS Data – For Discussion

20 August 2018
Prepared by: ICANN organization

A. Introduction

This paper is a working draft framework for a possible unified approach to allow continued access to full WHOIS data for authenticated users with a legitimate interest for accessing non-public WHOIS data consistent with the European Union's General Data Protection Regulation (GDPR). It builds from the discussion document published by ICANN organization on 18 June 2018 titled *Framework Elements for Unified Access Model for Continued Access to Full WHOIS Data* ("UAM Framework Elements")[1] as well as various inputs from the community[2] and the European Data Protection Board[3].

What is the purpose of this paper?

This working draft is intended to facilitate further discussions with the European Data Protection Board and the ICANN community about a unified access model. It outlines basic parameters of a possible unified access model based on ICANN org's current understanding of how the GDPR relates to such a model, to enable ICANN org to continue to seek input from the European Data Protection Board about what may or may not be permitted by the GDPR. Overall, guidance from the European Data Protection Board may increase legal certainty for data controllers about whether a unified access model could be implemented. This paper also includes some initial thoughts about process and technical questions that will need to be discussed as part of a unified access model.

This paper is purposefully written as a high-level framework to help understand the technical and legal foundation upon which a unified access model could potentially be built – not to design the final unified access model or discuss how it could be implemented. The details of any unified access model would require further and deeper community discussion and engagement.

There are some open questions where there are differing viewpoints in the community on the appropriate approach that should be incorporated into a final version of a unified access model. Another purpose for this paper is to identify those issues in order to seek specific guidance and facilitate focused discussions. These open issues are further outlined in **Section E**.

This paper and the work to obtain feedback from the community and the European data protection authorities does not replace the multistakeholder policy development process, including the ongoing Expedited Policy Development Process concerning the Temporary Specification for gTLD Registration Data, which includes as part of its charter work on a standardized access model after certain gating questions are resolved. Instead, it is anticipated that guidance and feedback from European data protection authorities as well as the ICANN

---

[1] https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-18jun18-en.pdf

[2] https://www.icann.org/resources/pages/gdpr-comments-2018-04-04-en; https://www.icann.org/resources/pages/gdpr-legal-analysis-2017-11-17-en#discussions

[3] https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf

community could serve as important data points to support the work of any policy development process.

Why now?

In this context, ICANN org is publishing this working draft paper about a possible unified access model at this time to help advance the discussion within the ICANN community while continuing to seek additional guidance from the European data protection authorities. As discussed in various ICANN blogs and during the ICANN62 meeting in Panama City, ICANN org continues to engage with European data protection authorities and the European Commission on these issues.

As noted in the background section below, there are several communications noting the interest and importance to develop a unified access model that complies with the GDPR in a timely manner. For example, community members have asked ICANN org to provide guidance about what may legally be permitted in a model so that this information can be factored into policy work. Also, those who regularly query WHOIS data, such as law enforcement authorities and intellectual property rights holders, are asking for more information about how to be qualified for predictable access to non-public WHOIS data. Moreover, those who are providing access to the non-public WHOIS data (registry operators and registrars) and those who receive access to the data are asking for greater legal clarity about their respective responsibilities in relation to the data.

B. Brief Summary of the Framework for a Possible Unified Access Model

A unified access model could potentially provide a standardized/predictable method for:

(1) third-parties with a legitimate interest for accessing personal data included in registration data to request access to such data from registry operators and registrars; and
(2) registry operators and registrars to have more legal certainty about how to ensure the appropriate balance between the third-party request for access to personal data included in registration data is not overridden by the fundamental rights and freedoms of individuals whose personal data is included in registration data.

As outlined in **Section F**, a third party that is part of an "eligible user group" could submit an application to an "accrediting body" to apply for credentials to be used to access non-public WHOIS data. If the application is approved by the authenticating body, the user would be required to agree to abide by Terms of Use that would include required measures to adequately safeguard the personal data that may be made available to the user. Violation of the Terms of Use could result in revocation of the user's credentials for access among other things.

To make a specific query for a domain name the user would take its credentials to the relevant registry operator or registrar to perform a query through an RDAP service. As part of its query, the user would be required to specify its purpose for accessing the data, and possibly agree to abide by the terms of an access agreement with the registry operator or registrar detailing any additional responsibilities as a recipient of personal data. The registry operator/registrar would validate the credentials with the authenticating body before providing a response to the user's query. Subject to applicable local laws, the registry operator/registrar would provide the user access to the non-public WHOIS data elements consistent with the legitimate purpose identified in the query. The user receiving the data takes on responsibility for its use of the data consistent with the Terms of Use as well as any access agreement.

The access model discussed in this paper attempts to provide an alternative, uniform method beyond legal due process for registry operators and registrars to provide continued access to full WHOIS data for legitimate purposes, but recognizes that such an approach may prove to be challenging given the legal parameters of the GDPR, requiring the balancing of legitimate interests with the interests, rights, and freedoms of affected data subjects. Developing a unified approach for proportionate data processing consistent with the GDPR while minimizing the risk of unauthorized and unjustified processing will continue to require careful consideration and consultation with the relevant data protection authorities to develop a legally sustainable solution.

Attachment 1 provides a high-level outline of the steps for a user to request access to non-public WHOIS data through a possible unified access model and includes questions that arise at each step that are relevant to registry operators/registrars, the authenticating bodies, and ICANN. The chart also includes references to specific sections of this paper where further details on a particular issue are provided. **Attachment 2** provides a diagram of the process.

C. Background

On 17 May 2018, the ICANN Board adopted the Temporary Specification for gTLD Registration Data ("Temporary Specification"). The Temporary Specification establishes temporary requirements to allow ICANN and gTLD registry operators and registrars to continue to comply with existing ICANN contractual requirements and community-developed policies concerning gTLD registration data (including WHOIS) in light of the GDPR. The Temporary Specification maintains robust collection of registration data (including Registrant, Administrative, and Technical contact information), but restricts most personal data to layered/tiered access. Users with a legitimate and proportionate purpose for accessing the non-public personal data are able to request such access through each of the 2,500+ gTLD registrars and registry operators. Under the Temporary Specification, registrars and registry operators are required to provide reasonable access to this data based on legitimate interests pursued by the third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the registrant or data subject.

Given that registrars and registry operators may have differing approaches as to how they meet the obligation of the Temporary Specification regarding access to non-public WHOIS data, ICANN and the community have been exploring whether it is possible to develop an automated "unified" approach across all gTLD registrars and registry operators for providing access to non-public WHOIS data in a manner that is consistent with the GDPR, including the obligations on data controllers.

When adopting the Temporary Specification, the ICANN Board identified some implementation issues raised during the course of development of the Temporary Specification for which the Board encouraged the community to continue discussing so that the issues could be resolved as quickly as possible. Among the items the Board identified were "work to develop an accreditation and access model that complies with GDPR, while recognizing the need to obtain additional guidance from the Article 29 Working Party/European Data Protection Board."

Additionally, various parts of the community, including governments and European data protection authorities have called for community work to develop a unified approach for accessing non-public WHOIS data. For example, in its 11 April 2018 letter, the Article 29 Working Party stated that it:

> *…expects ICANN to develop and implement a WHOIS model which will enable legitimate uses by relevant stakeholders, such as law enforcement, of personal data concerning registrants in compliance with the GDPR, without leading to an unlimited publication of those data. In this respect the WP29 encourages ICANN to develop appropriate policies and procedures applicable to incidental and systematic requests for access to WHOIS data, in particular for access by law enforcement entities.*[4]

Also, the European Commission invited ICANN "to consider and possibly integrate models for the accreditation system currently being developed by relevant stakeholders (e.g. by the business community). ICANN should take this opportunity to come up with a model that reflects not only compliance with the GDPR, but a genuine commitment to the spirit of the GDPR. At the same time, ICANN should be proactive, and ensure that the system will actually operate to mitigate risks of potential or actual harm to people and the security and stability of the Internet. This is a core part of ICANN's mission."[5]

In its Panama City Communiqué, the Governmental Advisory Committee (GAC) made note of "the negative impact that the lack of timely access to non-public WHOIS data is having on different user groups and expressed a desire to achieve more consistent and timely access." The GAC also offered specific advice to the Board to "[t]ake all steps necessary to ensure the development and implementation of a unified access model that addresses accreditation,

[4] https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf
[5] https://www.icann.org/en/system/files/correspondence/viola-et-al-to-marby-17may18-en.pdf

authentication, access and accountability, and applies to all contracted parties, as quickly as possible…."[6]

In its 5 July 2018 letter, the European Data Protection Board provided additional guidance to ICANN, noting that the guidance would "enable ICANN to develop a GDPR-compliant model for access to personal data processed in the context of WHOIS."

D. Important Note about Terminology

As part of the discussion in the community over the past several months about a possible unified access model, terms such as "accreditation," "authentication," "certification," and "code of conduct" have been used to discuss various elements of a model. Some of these terms (e.g. "code of conduct") have specific meaning in the context of the GDPR.

As noted in the 5 July 2018 letter from the European Data Protection Board, "codes of conduct certification and/or accreditation are voluntary measures, which controllers or other representative bodies may develop with a view of helping to demonstrate compliance with the provisions of the GDPR. Putting in place such measures is therefore not required by the GDPR." In other words, a unified access model designed to satisfy the requirements Articles 40 and 41 of the GDPR concerning codes of conduct and certification methods is one possible way, but not the only way, to develop an appropriate access model.

Currently, this paper does not propose to make use of the mechanisms in Articles 40 and 41 of the GDPR to underpin a unified access model but leaves open the possibility for further discussion by the community about whether such options should be explored. Additionally, ICANN org continues to separately explore whether there are "opportunities for ICANN, beyond its role as one of the 'controllers' with respect to WHOIS or its contractual enforcement role, to be acknowledged under the law as the coordinating authority of the WHOIS system."[7]

To provide clarity for future community discussions about a possible unified access model, this discussion paper uses the following terminology:

1. **Authentication** refers to the process of validating eligible individuals/entities for accessing non-public WHOIS data through a unified access model. Use of this term should not be confused with the formal accreditation process provided for in Article 42, GDPR.

2. **Terms of Use** refers to a set of safeguards that would be established for the use of non-public WHOIS data, including proper procedures for accessing data and limitations on use of the data. Authenticated users/user groups would be required to adhere to

[6] https://gac.icann.org/advice/communiques/icann62_gac_communique%CC%81-ar.pdf
[7] https://www.icann.org/news/blog/data-protection-privacy-update-icann-s-gdpr-efforts-with-temporary-specification-now-in-effect

applicable Terms of Use. This proposal currently does not propose to use the process under Article 40, GDPR for seeking approval of the Terms of Use as a code of conduct. As discussed further in **Section F, Question 16** the Terms of Use would be developed in consultation with the ICANN Governmental Advisory Committee (GAC) and the European Data Protection Board so that public policy considerations are appropriately taken into account.

3. **Non-public WHOIS data** includes personal data included in registration data elements required to be redacted from data publicly available in WHOIS, including the name and email address of the registrant.

4. **WHOIS** is used throughout this document for ease of reference but is intended to cover Registration Data Directory Services (RDDS) generally.

E. Community Views About High-Level Elements of a Unified Access Model

A review of access models submitted by the community as well as comments on ICANN's UAM Framework Elements suggests that there is convergence on some key elements of a possible unified access model, including using a Registration Data Access Protocol (RDAP)[8] service as the technical method for providing layered/tiered access to non-public WHOIS data. Also, there seems to be convergence for implementing strong safeguards, perhaps through access agreements or other terms of use, to prevent and combat abuse of non-public WHOIS data provided to authenticated users, as well using a "decentralized" process for developing criteria and methods for authenticating various types of users to allow for entities with relevant expertise to authenticate relevant user groups (i.e. having separate authenticating bodies for each type of eligible user group.)

Also, there seem to be some competing views on the legal requirements of the GDPR as they relate to a unified access model, namely:

1. whether or not an authenticated user requesting access to non-public WHOIS data must provide its legitimate interest for each individual query/request;

2. whether or not full WHOIS data must be returned when an authenticated user performs a query; and

3. whether or not logs of query activities concerning non-public data must be available to the registrant upon request except if prohibited by a relevant court order or legal requirement.

[8] https://www.icann.org/rdap

There also are competing viewpoints on certain key process elements of a unified access model, including:

4. whether or not both registrars and registry operators must be required to provide access to non-public registration data;

5. whether or not there should be a fee imposed for accessing non-public WHOIS data; and

6. whether or not there should be a centralized portal operated by ICANN from which authenticated users are able to perform queries of non-public WHOIS data.

These competing community views are discussed in additional detail in **Section F**.

F. Summary Description of a Framework for a Possible Unified Access Model

---

Eligibility

---

1. Who would be eligible for continued access for WHOIS data via a unified access model?

Only a defined set of user groups with legitimate interests who are bound by Terms of Use requiring adequate measures of protection would be eligible for access to non-public WHOIS data via a unified access model. Registry operators and registrars would continue to be required to provide reasonable access to other third parties on the basis of a legitimate interests pursued by the third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Registered Name Holder or data subject pursuant to Article 6(1)(f) GDPR.

Some comments from the community suggest that work to define a list of specific categories of users that would be eligible to use a unified access model is not an approach that should be taken to develop a unified access model because it is a secondary issue and detracts from the primary issue of ensuring that rights of data subjects are at the forefront, which should be the principal concern of the model.

The model described in this paper incorporates the concept of defining eligible user groups to attempt to strike a balance between potential third party users who may request access to non-public WHOIS data on a regular basis where additional safeguards and process may be required or warranted, versus those who may request non-public WHOIS data on a more limited or one-off basis. Other elements discussed in the framework, including ensuring there are Terms of

Use with adequate measures of protecting and safeguarding personal data, are designed to make sure that data subjects rights are adequately protected.

2. Who would determine eligibility?

At the outset, governments within the European Economic Area (who also are members of the GAC) would identify or facilitate identification of broad categories of eligible user groups ("Eligible User Groups"). Building from this guidance, ICANN org would engage with other governments through the GAC to identify specific Eligible User Groups. For example, Eligible User Groups might include intellectual property rights holders, law enforcement authorities, operational security researchers, and individual registrants.

This feature is intended to ensure that public policy considerations are duly taken into account when defining which groups should be eligible for access via a unified access model.

3. How would authentication requirements for legitimate users be developed?

For law enforcement authorities, individual governments would determine authentication requirements for who should be granted access from their respective jurisdictions. This information would be communicated via the GAC. As noted in the 11 April 2018 letter[9] from the Article 29 Working Party, there could potentially be a role for Interpol or Europol to serve as the global body to help determine the authentication requirements for law enforcement authorities. The Article 29 Working Party notes that, "[t]he 'accreditation' for incidental or systematic access to WHOIS data by law enforcement agencies might be arranged through for example Interpol or Europol, to help registry operators and registrars globally to ascertain the accreditation of such an agency, provided this can be done in accordance with the applicable legal frameworks."[10] ICANN org will continue to request additional clarification from the European Data Protection Board about the "applicable legal frameworks" referenced in the 11 April letter as additional guidance on this point was not addressed in the European Data Protection Board's most recent letter to ICANN of 5 July 2018.

For private third parties, ICANN would consult with the GAC and members of the Eligible User Groups to identify relevant bodies with expertise to authenticate users within an Eligible User Group (the "Authenticating Bodies"), and the Authenticating Bodies would develop criteria to authenticate individual users within an Eligible User Group.

Some parts of the community have begun discussions in this regard, and for example, have identified WIPO or a similar party as the administrator of the Trademark Clearinghouse as possible Authenticating Bodies for intellectual property rights holders.

[9] https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf
[10] https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-10may18-en.pdf

Additionally, there would be specific user groups who are automatically approved for access via a unified access model for specific legitimate purposes – namely, ICANN for the purpose of contractual compliance enforcement, ICANN-related dispute resolution providers, and registrars for the purpose of facilitating the transfer of domain names.

This paper suggests a "decentralized" approach for Authenticating Bodies to allow for entities with an appropriate level of expertise in relation to the subject-matter of the Eligible User Group to develop the authentication requirements for the group.

An additional matter that would require further discussion and consideration is the scope of responsibility for the Authenticating Body with respect to the users they authenticate. For example, would an Authenticating Body have some level of legal responsibility if an authenticated user abuses its access rights or there is finding that the Authenticating Body's authentication standards are not rigorous enough to avoid gaming or prevent abuse?

Process Details

---

4. **Who would be required to provide access to non-public WHOIS data?**

Both registry operators and registrars would be required to provide access to non-public WHOIS data under a unified access model to authenticated users.

Some comments from the community propose that registrars, but not registry operators, should be required to provide access to non-public WHOIS data under a unified access model. These comments note that registrars are the entities with the direct contractual relationship with the registrant, and thus are in a better position to protect registrant data from abuse and unauthorized use.

This paper takes that position that discussions about whether only registrars should be required to provide access to non-public WHOIS, for example, would be a possible topic for discussion in any relevant policy development process.

5. **What would be the overall process for authenticating legitimate users for access non-public WHOIS data under a unified access model?**

A third party with a legitimate interest for accessing non-public WHOIS data would submit to the approval process required by the relevant Authenticating Body, which could include an application process for example. If the user successfully satisfies the requirements of the Authenticating Body, the user would be required to confirm its adherence to the relevant Terms of Use, which is discussed in additional detail below.

The Authenticating Body would provide the required credentials to be presented to the registry operator or registrar to access non-public WHOIS data.

To gain access to the non-public WHOIS data, the authenticated user would present its credentials to the relevant registry operator or registrar and identify its legitimate purpose for requesting access to the non-public WHOIS data. The registry operator or registrar would verify the credentials with the Authenticating Body, evaluate the request, and the authenticated user would be provided query-based access to non-public WHOIS data as appropriate. There is a question about whether the authenticated user would be required to enter into some type of "access" agreement with the registry operator or registrar above and beyond the Terms of Use.

6. What scope of data would be available to authenticated users?

Authenticated users would be granted query-based access to the level/scope of non-public WHOIS data consistent with the identified legitimate purpose presented to the registry operator or registrar for each query.

Some comments from the community suggest that full WHOIS data should be returned if a query is made by an authenticated user given that the user would have successfully completed the authentication process and would be bound to abide by Terms of Use (see Question 14 for further discussion of Terms of Use). Others suggest that the GDPR would not permit an access model based on "trust" of an authenticated user adhering to Terms of Use. Instead, they suggest that the model must be built around the idea that an authenticated user must nevertheless have a legitimate interest to access a specific WHOIS record for a specific and identified purpose.

In its 5 July 2018 letter, the European Data Protection Board advised that:

> *ICANN and the registrars/registries are, as controllers, responsible for ensuring that personal data processed in the context of WHOIS are only disclosed to third parties with a legitimate interest or other lawful basis under the GDPR, also taking into account the other requirements of the GDPR. This implies putting in place an appropriate access model, with appropriate safeguards, including measures to ensure a sufficient degree of compliance assurance.*

In light of the guidance from the European Data Protection Board and ICANN org's current understanding of the responsibilities of ICANN, registrars, and registry operators as data controllers for certain processing activities related to WHOIS, this paper takes the position that access to non-public WHOIS data would be on a query-by-query basis, and that it would not be permissible to provide the full WHOIS record by default to an authenticated user, unless doing so would be supported by the legitimate interest provided by the authenticated user.

ICANN org will seek guidance from the European Data Protection Board about whether it would be consistent with the obligations of the data controllers under the GDPR (perhaps through

additional safeguards) to have an access model that would allow for access beyond individual queries (e.g. bulk requests for access), and to full WHOIS data by default for authenticated users.

7. **Would registry operators and registrars be required to provide access to non-public WHOIS data to all authenticated users?**

Registry operators and registrars would be required to provide global access to authenticated users consistent with the identified legitimate purpose, and subject to applicable local laws. This feature is included based on obligations of data controllers under GDPR to ensure that the data processing is proportionate to the identified purposes.

8. **Would a unified access model incorporate transparency requirements?**

Yes, a unified access model would incorporate transparency requirements. For example, each Authenticating Body would maintain, but not publish, a list of the authenticated users so that appropriate monitoring and auditing could occur.

Additionally, based on guidance provided in the 5 July 2018 letter from the European Data Protection Board, registrars would be required to maintain audit logs of domain name queries for non-public WHOIS data, unless logging a particular entry is prohibited by law. The logs would include information such as the domain name being queried, the authenticated user querying the data, and the purpose identified for requesting access to the data.

Including logging requirements as part of a possible unified access model is based on guidance provided in the European Data Protection Board's letter, which states:

> *The EDPB considers that, unless there is an explicit prohibition in national law, appropriate logging mechanisms should be in place to log any access to non-public personal data processed in the context of WHOIS. In this context, such logging is considered required as part of the security obligation of controllers (article 32), as well as the obligation and in order to be able to demonstrate compliance with the GDPR (accountability) (article 5(2))… It is up to ICANN and other controllers participating in the WHOIS system to ensure that logging information is not disclosed to unauthorized entities, in particular with a view of not jeopardizing legitimate law enforcement activities.*

ICANN org proposed that the logs would be available to ICANN org for audit/compliance purposes, relevant data protection authorities, or pursuant to a court order. Additionally, the logs would be available to registrants by request (i.e. not automatically pushed out) given that "[d]ata subject rights, including the right of access, must however be accommodated unless one of the exceptions under the GDPR applies or if national legislation provides for a restriction in accordance with the GDPR (article 23)." One factor that would require further consideration is

how to balance data subject rights with individual WHOIS users whose personal data may be logged as part of a query for non-public WHOIS data.

In light of the guidance provided by the European Data Protection Board concerning logging obligations (as well as guidance discussed in Question 6) it is not clear that searchable WHOIS functionality for non-public WHOIS data would be consistent with these accountability requirements of the GDPR. ICANN org proposes to seek further guidance from the European Data Protection Board on this matter to better understand what may be permitted.

9. Would there be any fees as part of a unified access model?

Access models presented by some community members include the possibility of application fees to become an authenticated user to offset the cost of the Authenticating Body's evaluation of an application. Others have suggested that authenticated users should be required to pay nominal fess to access non-public WHOIS data because the current system unfairly requires (i) registrars and registry operators to bear the cost for providing a WHOIS service, and (ii) registrants to bear the cost of using privacy/proxy services if they do not want their personal contact details to appear in WHOIS.

Other comments, however, suggest that no fees should be imposed for accessing non-public WHOIS data (unless decided through a Policy Development Process) given that WHOIS is a critical service provided in the public interest (as a public resource) for a variety of legitimate uses. Additionally, discussions including at ICANN's meeting in Panama noted the importance of ease of use and affordability to the global community.

ICANN org takes note of the differing views on this topic and suggests that the financial implications of a possible unified access model would continue to require further study to assess this issue.

10. Would there be a process to review the effectiveness of a unified access model?

Yes, a unified access model would be reviewed at regular intervals to identify efficiencies and improvements to the implementation of the model.

Technical Details

---

11. Would there be a central repository of WHOIS data from which access would be granted to authenticated users?

No, registrars and registry operators would maintain current requirements to operate a WHOIS service.

Some comments suggested that there should be a centralized repository of WHOIS data from which access could be granted. They note that having a centralized system may have several benefits, including ease of use, efficiencies in delivering WHOIS services, and the ability to monitor and mitigate against possible abuse. Some comments recommend that even if there is no centralized WHOIS database, there should be a central portal (operated by ICANN) from which authenticated users would perform WHOIS queries so that users would not be required to go to individual registrar or registry operators for the data. ICANN org will continue to evaluate this proposal for possible discussion in future iterations of this paper, including potential security and legal implications of a centralized database or portal.

12. What technical method would be required to provide access to non-public WHOIS data?

Registry operators and registrars would be required to provide access to non-public WHOIS data via a Registration Data Access Protocol (RDAP) service. As previously noted, the comments from the community seem to suggest that there is convergence on the idea that RDAP should be used for a unified access model.

13. What technical method would be used to authenticate users?

This paper proposes that a possible unified access model would rely on a system of credentials as the technical method for identifying authenticated users.

Access models proposed by some community members also generally propose to rely upon a system of credentials, tokens and/or certificates to identify authenticated users. Some community models include more details about specific token or certificate mechanisms that should be used in an access model.

Terms of Use for Accessing Non-Public WHOIS Data

---

14. What would be the role of Terms of Use in a unified access model?

Terms of Use would establish a framework for the use of non-public WHOIS data by authenticated users accessing non-public WHOIS data through a unified access model, and in particular appropriate limitations on the use of such data, proper procedures for accessing the data, and other safeguards and public policy considerations relating to the responsibilities and practices for the Eligible User Groups.

In general, the non-public WHOIS data must be used for the purposes it was provided, and it must not be forwarded to unauthorized third parties.

15. Would there be multiple Terms of Use?

Yes, this paper suggests the possibility that a unified access model would include separate Terms of Use for each Eligible User Group to pursue a tailored and balanced approach regarding these groups and taking into account differing user interests. There would therefore be some safeguards that are common across all Terms of Use, whereas other safeguards would be specific to the Eligible User Group.

16. How would the Terms of Use be developed?

In consultation with the GAC and the European Data Protection Board, ICANN org would develop the standardized terms and safeguards common to be included across all Terms of Use. As provided in the GAC's San Juan Communiqué, the GAC "does not envision an operational role in designing and implementing the proposed accreditation programs but reiterates its willingness to advise the Board and engage with ICANN Org and the community in the development of codes of conduct from a public policy perspective."

The Authenticating Body for each Eligible User Group would be responsible for developing additional safeguards specific to the relevant Eligible User Group, which would be incorporated in the Terms of Use.

17. What types of safeguards would be included in the Terms of Use?

Among other things, the Terms of Use would include the following types of safeguards:

a. Appropriate limitations on use of the data;
b. Proper procedures for accessing the data, including appropriate limitations on query volume to prevent abuse;
c. Security measures for accessing the data;
d. Limitations on onward transfers of the data;
e. Safeguards for data subject rights;
f. General data protection obligations of the data controllers;
g. Fair and transparent processing requirements; and
h. Other safeguards and public policy considerations relating to the responsibilities and practices for the Eligible User Group.

Some additional safeguards suggested in comments from the community include: penalties for abuse/non-compliance with safeguards, and a recourse mechanism, such as an alternative dispute resolution mechanism, to allow recourse for registrants against users who have abused the unified access model.

An additional safeguard identified in some feedback from the community was appropriate rate limiting of queries for non-public WHOIS data. While rate limiting could serve to prevent abuse of a unified access model, comments suggest that such limitations could also harm legitimate

law enforcement investigations or the work of security practitioners. Additional discussion with the community is needed to address this matter.

18. What mechanism would be used to require compliance with the Terms of Use?

Authenticated users would be required to declare adherence to the relevant Terms of Use, either through an agreement with the Authenticating Body or some other method binding the user to comply with the Terms of Use.

Some of the access models proposed by community members include drafts of access agreements that could be considered as part of future discussions about an access model.

19. Who would monitor and enforce compliance with Terms of Use?

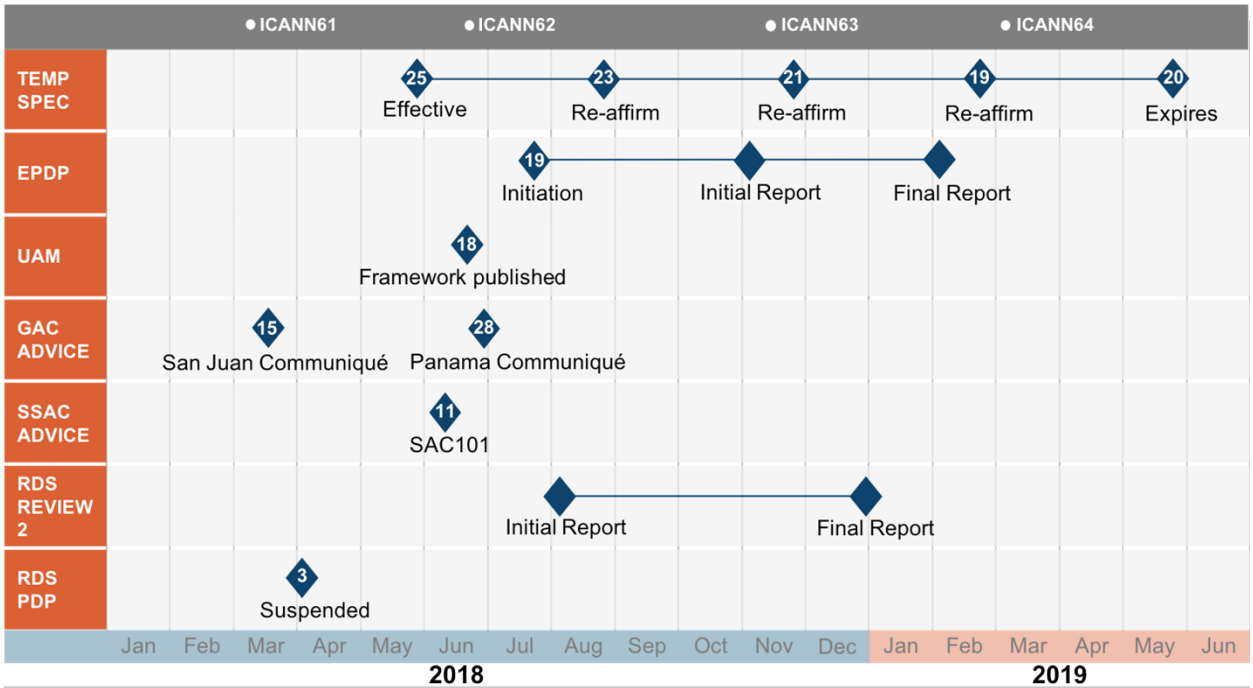
The Authenticating Body would monitor and enforce compliance with the relevant Terms of Use. ICANN org would develop a Memorandum of Understanding or Agreement with each Authenticating Body to ensure appropriate oversight consistent with ICANN's mission stipulated in the Bylaws.

If a unified access model becomes a part of ICANN's agreements with registrars and registry operators, for example through adoption of a consensus policy or contract amendments, compliance issues concerning registry operators' or registrars' adherence to the requirements of a unified access model would be handled by ICANN's Contractual Compliance department.

G. Next Steps

ICANN org looks forward to receiving input from the community on this proposal, which can be submitted at gdpr@icann.org. As previously noted, ICANN org also intends to share this proposal with the European Data Protection Board to seek further guidance, in particular on areas where there are differing views in the community. We will seek to provide the next iteration of this proposal at the earliest time possible in light of the interest for a unified access model, while coordinating closely with the work of the Expedited Policy Development Process concerning the Temporary Specification.

A high-level timeline is provided to show the various tracks of work in the community concerning this work.



Temp Spec: Temporary Specification for gTLD Registration Data
EPDP: Temp Spec Expedited Policy Development Process
UAM: Unified Access Model
GAC Advice: Governmental Advisory Committee Advice
SSAC Advice: Security Stability Advisory Committee Advice
RDS Review 2: Registration Directory Services Review 2
RDS PDP: gTLD Registration Directory Services Policy Development Process

Attachment 1 – Draft High-Level Steps to Request Non-Public WHOIS Data via a Possible Unified Access Model

Third-party user	Registry operator/ Registrar	Authenticating Body	ICANN	Relevant Section of Proposal
Authentication process				
1. User submits application for authenticated access	• As a data controller, are there any agreements/arrangements needed with the Authenticating Bodies?	• Is Authenticating Body verifying a user's qualification as part of an "eligible user group" or are there other matters the Authenticating Body must evaluate? • Is there an application fee paid by user to cover the cost of evaluating the application and enforcing the Terms of Use?	• As a data controller, are there any agreements/arrangements needed with Authenticating Body?	Refer to Questions 1 – 3 for additional discussion of these issues.
2. Authenticating Body reviews application. If approved, requires user to agree to Terms of Use and issues credentials to user	N/A	• Must the Authenticating Body actively monitor compliance with the Terms of Use? • Would enforcement be coordinated with registry operator/registrar/ICANN?	• Would ICANN audit Authenticating Bodies to ensure standards are being met?	Refer to Questions 5, 8, 9, 15, 16, 18, 19 for additional discussion of these issues.

Third-party user	Registry operator/ Registrar	Authenticating Body	ICANN	Relevant Section of Proposal
<u>Specific request for access</u>				
3. User takes credentials to registry operator or registrar. User identifies legitimate interest as part of information submitted to perform a query. The registry operator/registrar validates credentials with the Authenticating Body	• Should user be able to perform query at both registry operator and registrar, or only the registrar? • Is it sufficient for user to check a box identifying its legitimate interest or is additional proof/documentation required (e.g. would a trademark rights holder be required to present a copy of its trademark registration if requesting access to non-public WHOIS data for the purpose of combating alleged trademark abuses?) • Must the user identify a separate legitimate interest for each query?	• Must the registry operator/registrar validate credentials with Authenticating Body for each query or is this a one-time process?	• Instead of requiring user to go to registry operator or registrar to perform query, should ICANN operate a central RDAP look-up from which all users perform queries?	Refer to Questions 5, 7, 11 – 13 for further discussion of these issues.
4. User submits query via RDAP	• Would it be permissible to develop an access system that allows for bulk access or search functionality?	• Because of its role for enforcing the Terms of Use what is the scope of responsibility for	• In ICANN's coordination role of the WHOIS system, what is its responsibility with respect to queries for	Refer to Questions 5, 6, 8 and 9 for further

Third-party user	Registry operator/ Registrar	Authenticating Body	ICANN	Relevant Section of Proposal
	• Can the registry operator/registrar rely on the balancing of interests developed as part of a unified access model or must each query be evaluated on case-by-case basis? • Must the registry operator/registrar keep a log of the query? • If registry operator/registrar is asked for a copy of the log from the registrant, law enforcement, or other third party must it be provided? • Would the user be required to submit a fee to access the non-public WHOIS data?	Authenticating Bodies for specific queries?	access to non-public WHOIS data?	discussion of these issues.
5. User receives a response to its query	• As a data controller, must there also be binding commitments above and beyond the Terms of Use signed between the Authenticating Body and	• Because of its role for enforcing the Terms of Use, what is the scope of responsibility for Authenticating Bodies for specific queries?	• In ICANN's coordination role of the WHOIS system, what is its responsibility with respect to queries for access to non-public WHOIS data?	Refer to Questions 6 – 8 for further discussion of these issues.

Third-party user	Registry operator/ Registrar	Authenticating Body	ICANN	Relevant Section of Proposal
	the user (e.g. an access agreement)? • What responsibilities attach to the user as a condition of the registry operator/registrar providing access to the non-public WHOIS data? • Would registry operator/registrar be permitted to return the full WHOIS record for all authenticated queries or must they further tier the data based on the legitimate purpose identified?			

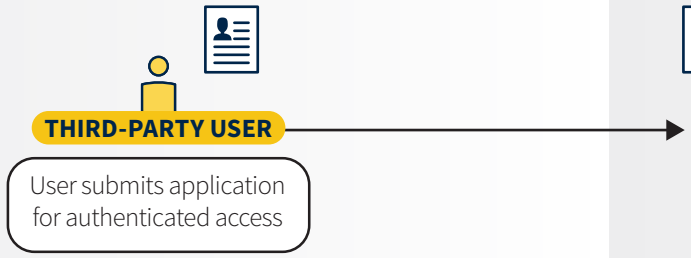
Attachment 2 – Diagram of Potential Process for Accessing Non-Public WHOIS Data Through a Unified Access Model

Working Draft of a Possible Unified Access Model AS OF 20 AUGUST 2018

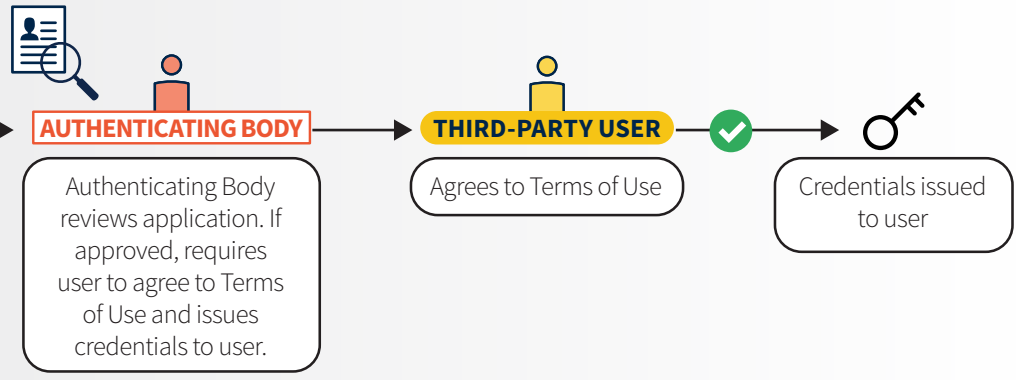
ICANN

Authentication Process

Step 1



Step 2



Relevant Questions - Step 1

REGISTRIES/REGISTRARS

N/A

AUTHENTICATING BODY

- Does the Authenticating Body verify or evaluate eligible user group's qualifications?
- Application fee?

ICANN ORG

- Are there agreements / arrangements with Authenticating Body?

REFER TO

- Questions **1 – 33** of the Proposal

Relevant Questions - Step 2

REGISTRIES/REGISTRARS

- Any agreements/arrangements with Authenticating Bodies?
- Does the user check a box identifying its legitimate interest or is additional proof / documentation required?
- Does the user identify a separate legitimate interest for each query?
- Is it permissible to develop an access system that allows for bulk access or search functionality?

AUTHENTICATING BODY

- What is the scope of responsibility for Authenticating Bodies for specific queries?

ICANN ORG

- What is ICANN's responsibility with respect to queries for access to non-public WHOIS data?

REFER TO

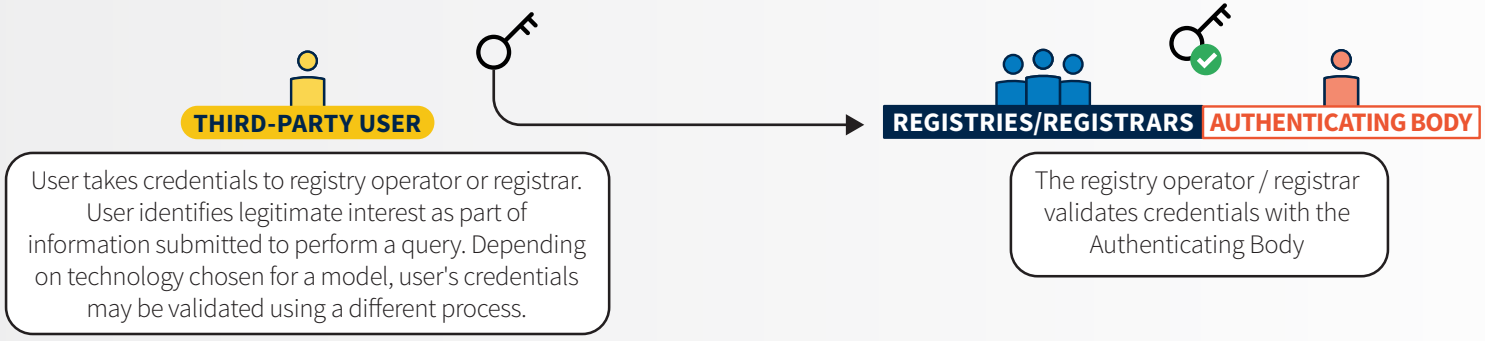
- Questions **5, 8, 9, 15, 16, 18, 19** of the Proposal

Working Draft of a Possible Unified Access Model AS OF 20 AUGUST 2018

ICANN

Specific Request for Access

Step 3



Relevant Questions - Step 3

REGISTRIES/REGISTRARS

- Could the user query at both the registry operator and registrar, or only registrar?

AUTHENTICATING BODY

- Does the registry operator / registrar validate token/credential with the Authenticating Body for each query, or is this a one-time process?

ICANN ORG

- Should ICANN operate a central RDAP look-up from which all users perform queries?

REFER TO

- Questions **5, 7, 11 – 13** of the Proposal

Working Draft of a Possible Unified Access Model AS OF 20 AUGUST 2018

ICANN

Specific Request for Access (continued)

Step 4

Relevant Questions - Step 4

REGISTRIES/REGISTRARS

- Should the registry operator / registrar rely on the balancing of interests or each query be evaluated on case-by-case basis?
- Should the registry operator / registrar keep a log of the query?
- Must the registry / registar provide a copy of the log if asked by a law enforcement or other third party?
- Should the user submit a fee to access the non-public WHOIS data?

AUTHENTICATING BODY

- What is the scope of responsibility for Authenticating Bodies for specific queries?

ICANN ORG

- What is ICANN's responsibility with respect to queries for access to non-public WHOIS data?

REFER TO

- Questions 8–9 of the Proposal

Step 5

Relevant Questions - Step 5

REGISTRIES/REGISTRARS

- Are there commitments above and beyond the Terms of Use signed between the Authenticating Body and the user?
- What are the user responsibilities as a condition of the registry operator / registrar providing access to the non-public WHOIS data?
- Should the registry operator / registrar be permitted to return the full WHOIS record for all authenticated queries or tier the data based on the legitimate purpose identified?

AUTHENTICATING BODY

- What is the scope of responsibility for Authenticating Bodies for specific queries?

ICANN ORG

- What is ICANN's responsibility with respect to queries for access to non-public WHOIS data?

REFER TO

- Questions 6–8 of the Proposal