Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS)

STATUS OF THIS DOCUMENT

This is the final report from the Expert Working Group on gTLD Directory Services (EWG), detailing our recommendations to the ICANN Board for a next-generation Registration Directory Service (RDS) to replace today's WHOIS system.

I. EXECUTIVE SUMMARY

This Final Report from the Expert Working Group on gTLD Directory Services (EWG) details our recommendations to ICANN's President/CEO and Board of Directors for a next-generation Registration Directory Service (RDS) to replace the current WHOIS system.

This Final Report represents the culmination of an intense 15+ month period of work during which this diverse group of volunteers spent thousands of hours on in-depth research, considered over 2600 pages of public comments, survey responses, and research results, and participated in 19 public community consultations, 35 days of face-to-face EWG meetings, 42 EWG calls, more than 200 subteam calls, and countless input-gathering sessions with outside experts and community members – all to answer a simple question:

Is there an alternative to today's WHOIS to better serve the global Internet community?

Yes, there is. The EWG unanimously recommends abandoning today's WHOIS model of giving every user the same entirely anonymous public access to (often inaccurate) gTLD registration data.

Instead, the EWG recommends a paradigm shift to a next-generation RDS that collects, validates and discloses gTLD registration data for permissible purposes only.

While basic data would remain publicly available, the rest would be accessible only to accredited requestors who identify themselves, state their purpose, and agree to be held accountable for appropriate use.

The next 150+ pages describe the input and research that led the EWG to this recommendation, a detailed proposal for a new RDS, and the following conclusions:

- This issue is very complex.
- The EWG has examined this issue from a multitude of perspectives and has conducted research to ensure the proposed RDS is implementable.
- The proposed RDS, while not perfect, reflects carefully crafted and balanced compromises with interdependent elements that should not be separated.
- The proposed RDS is designed to tackle, head-on, in an unprecedented manner:
    - Difficult data privacy issues;
    - Validation challenges that have long degraded data quality and accuracy; and

- Striking a workable balance between access and accountability.

- The RDS should be adopted as a whole. Adopting some but not all of the design principles recommended herein undermines benefits for the entire ecosystem.

This Final Report, including its recommendations and proposed principles for the next-generation RDS, reflects a consensus. This support is noteworthy given the wide range of perspectives and stakeholders reflected among the EWG members.[1]

The EWG is confident that this Final Report fulfills the ICANN Board's directive to help redefine the purpose and provision of gTLD registration data, providing a solid foundation to help the ICANN community (through the Generic Names Supporting Organization, GNSO) create a new global policy for gTLD directory services.

The EWG is confident that the RDS described in this Final Report provides a more solid foundation than exists today – a foundation from which the GNSO can develop a new global policy for gTLD registration data to protect personal privacy and ensure greater accuracy, accountability, and transparency for the entire ICANN ecosystem for years to come.

As the Board, the GNSO, and the ICANN community consider this Final Report, the EWG recommends that consideration be framed by the following questions:

- Is the RDS preferable to today's WHOIS?
- If not, does the ICANN community agree that the current WHOIS system should continue, and can it meet the needs of the evolving, global Internet?

Background

The EWG was formed by ICANN's CEO, Fadi Chehadé, at the request of ICANN's Board, to help resolve the nearly decade-long deadlock within the ICANN community on how to replace the current WHOIS system.[2]

To move beyond WHOIS deficiencies identified by numerous community reports and studies[3], the EWG's mandate is to re-examine and define the purpose of collecting and maintaining gTLD registration data, consider how to safeguard the data, and propose a next-generation solution that will better serve the needs of the global Internet community.

---

[1] Please see Annex J for the composition of the EWG and member expertise.

[2] Refer to https://www.icann.org/news/announcement-2-2012-12-14-en

[33] Refer to Annex B for a list of reports that document deficiencies in WHOIS.

Starting with a tabula rasa, the EWG questioned fundamental assumptions about the purposes, uses, collection, maintenance and provision of registration data. The EWG considered each stakeholder involved in gTLD directory services, examining their needs for accuracy, access, and privacy. It considered possible approaches to meet those needs more effectively.

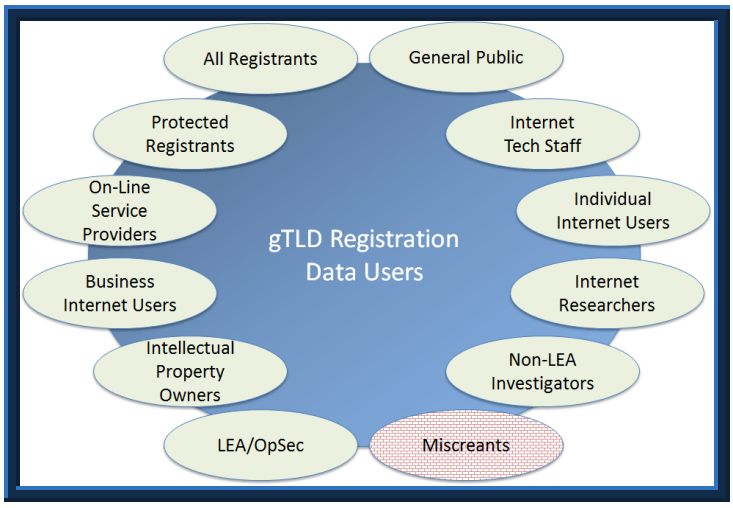
To guide its deliberations, the EWG developed a high-level statement of purpose, using it to align this report's recommendations with ICANN's mission and design a system to support domain name registration and maintenance which:

- Provides appropriate access to accurate, reliable, and uniform registration data;
- Protects the privacy of Registrant information;
- Enables a reliable mechanism for identifying, establishing and maintaining the ability to contact Registrants;
- Supports a framework to address issues involving Registrants, including but not limited to: consumer protection, investigation of cybercrime, and intellectual property protection; and
- Provides an infrastructure to address appropriate law enforcement needs.

Users and Purposes

The EWG examined existing and potential purposes for collecting, storing, and providing gTLD registration data to a wide variety of users, examining an extensive, representative set of actual WHOIS use cases.

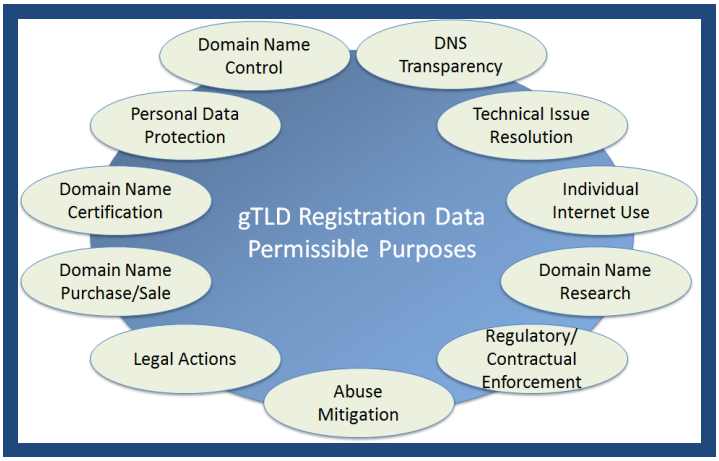
The EWG considered the totality of these use cases and the lessons learned from them, as well as reference material and community input, to derive a consolidated set of users and permissible purposes that must be accommodated by the RDS and potential misuses that must be deterred.



Purposes to be Accommodated or Prohibited

Consistent with the EWG's mandate, all of these users were examined to identify existing and possible future workflows and the stakeholders and data involved in them.

Domain name registration information needs were analyzed to derive mandatory data elements, related risks, privacy law and policy implications, and address other questions explored in this report. The EWG's recommended permissible purposes are summarized at right.

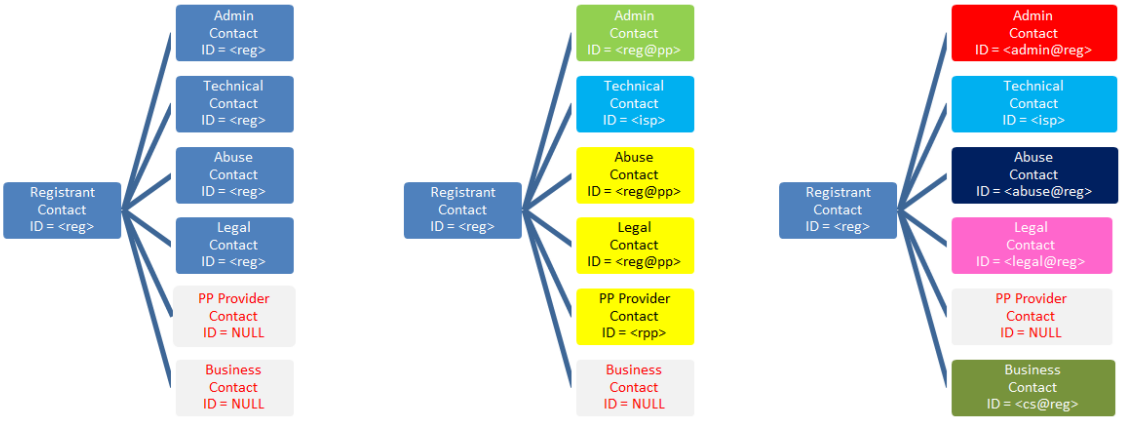


Currently-identified permissible purposes and associated registration data, contact, and query needs are defined below and further detailed in Section III.

Purpose	Includes tasks such as…
Domain Name Control	Creating, managing and monitoring a Registrant's own domain name (DN), including creating the DN, updating information about the DN, transferring the DN, renewing the DN, deleting the DN, maintaining a DN portfolio, and detecting fraudulent use of the Registrant's own contact information.
Personal Data Protection	Identifying the accredited Privacy/Proxy Provider or Secure Protected Credential Approver associated with a DN and reporting abuse, requesting reveal, or otherwise contacting that Provider.
Technical Issue Resolution	Working to resolve technical issues associated with domain name use, including email delivery issues, DNS resolution failures, and website functional issues, by contacting technical staff responsible for handling these issues.
Domain Name Certification	Certification Authority (CA) issuing an X.509 certificate to a subject identified by a domain name needing to confirm that the DN is registered to the certificate subject.
Individual Internet Use	Identifying the organization using a domain name to instill consumer trust, or contacting that organization to raise a customer complaint to them or file a complaint about them.

Purpose	Includes tasks such as…
Business Domain Name Purchase or Sale	Making purchase queries about a DN, acquiring a DN from another Registrant, and enabling due diligence research.
Academic/Public-Interest DNS Research	Academic public-interest research studies about domain names published in the RDS, including public information about the Registrant and designated contacts, the domain name's history and status, and DNs registered by a given Registrant.
Legal Actions	Investigating possible fraudulent use of a Registrant's name or address by other domain names, investigating possible trademark infringement, contacting a Registrant/Licensee's legal representative prior to taking legal action and then taking a legal action if the concern is not satisfactorily addressed.
Regulatory and Contractual Enforcement	Tax authority investigation of businesses with online presence, UDRP investigation, contractual compliance investigation, and registration data escrow audits.
Criminal Investigation & DNS Abuse Mitigation	Reporting abuse to someone who can investigate and address that abuse, or contacting entities associated with a domain name during an offline criminal investigation.
DNS Transparency	Querying the registration data made public by Registrants to satisfy a wide variety of needs to inform the general public.

To deliver purpose-based access to registration data while improving communication and personal privacy, the EWG developed principles for Purpose-Based Contacts (PBCs). Supported by defined roles and responsibilities, PBCs have been mapped to all permissible purposes where contact is needed. Three examples are illustrated below and further detailed in Sections III and IV.



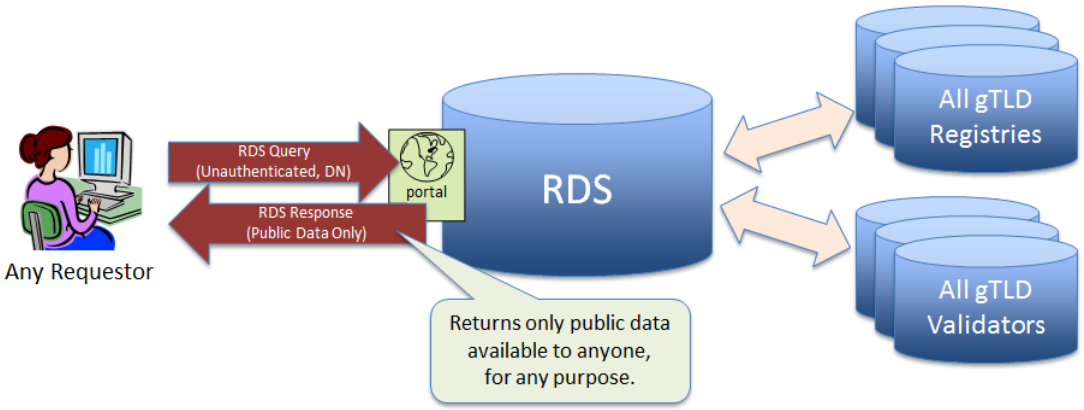
The EWG further analyzed all registration data elements – starting from those defined in the 2013 RAA – to derive a set of guiding principles for data collection and disclosure which dovetails with the recommended PBC framework, as well as with recommendations made to enable compliance with data protection laws. The EWG made further recommendations to identify new data elements that Registrants and contacts may choose to publish to make communication more robust. These recommendations are detailed in Section IV and examples given in Annex E.

Purpose-Driven Access

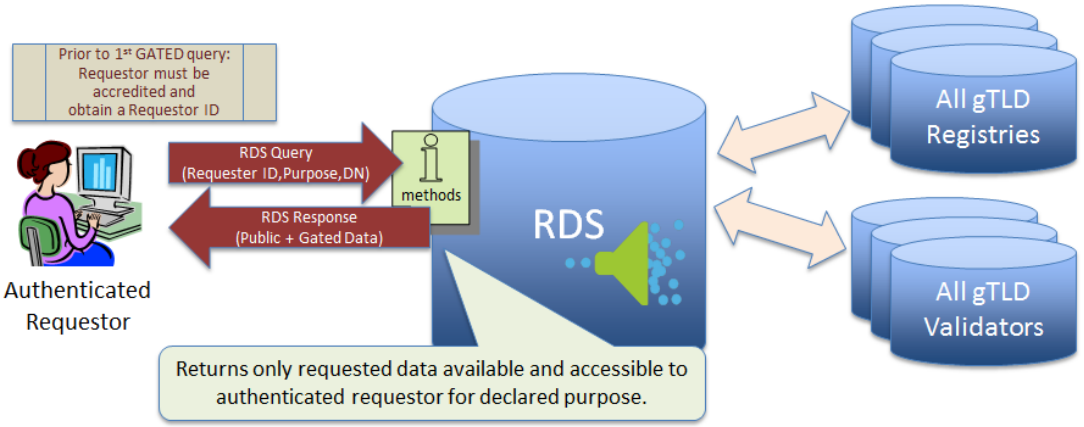
The recommended RDS takes a clean slate approach, abandoning today's one-size-fits-all WHOIS in favor of purpose-driven access to validated data in hopes of improving privacy, accuracy and accountability. The EWG believes that this new access paradigm could increase accountability for all parties involved in the disclosure and use of gTLD domain name registration data by:

- Logging all access to gTLD registration data, including unauthenticated access to public data elements, to enable detection and mitigation of abuses;
- Gating access to more sensitive data elements that would only be available to requestors who applied for and were accredited to receive RDS access, at the level appropriate for each user and stated purpose; and
- Auditing both public and gated data access to minimize abuse and impose penalties and other remedies for inappropriate use, in accordance with terms and conditions explicitly agreed upon by each requestor.

The EWG's Principles for Data Access, which served as the bases for its detailed recommendations on public and gated data access, are detailed in Section IV. As depicted below, public data elements can still be requested from the RDS by anyone, with or without authentication.



Gated data elements can also be requested via the RDS. To do so, requestors must first be accredited. Thereafter, requestors may submit authenticated queries requesting data elements for a stated purpose.



Refer to Annex E for a more detailed illustration of data elements returned to both public and gated data queries, how gated access depends upon the user and purpose, and how RDS User Accreditors might play a role in authorizing and auditing gated access.

Privacy and Data Protection

Central to the remit of the EWG is the question of how to design a system that increases the accuracy of the data collected while also offering protections for those Registrants seeking to guard and maintain their privacy.

The EWG recognizes that personal information is protected by data protection law, and that even where there is no law, there are legitimate reasons for individuals to seek heightened protections of their personal information. In addition, some businesses and organizations may seek protection of their information for legitimate purposes, such as when they are preparing to launch a new product line, or, in the case of small business, where contact information discloses personal data.

Accordingly, the EWG formulated a set of recommendations to enable routine compliance with privacy and data protection laws, detailed in Section VI. These principles cover:

- Mechanisms to facilitate routine legally compliant data collection and transfer between actors within the RDS ecosystem;
- Standard contract clauses that are harmonized with privacy and data protection laws and codified in policy;
- A "rules engine" to apply data protection laws; and
- How RDS data storage location relates to law enforcement access.

In addition to the privacy afforded by compliance with data protection laws, the RDS also recommended principles to accommodate needs for privacy by including within the RDS ecosystem:

- An accredited Privacy/Proxy Service for general use; and
- An accredited Secure Protected Credentials Service for persons at risk and in instances where free speech rights may be denied or speakers persecuted.

The EWG further recommends that ICANN investigate the development of a single, harmonized privacy policy that governs RDS activities in a comprehensive manner.

To address needs for more uniform and reliable Privacy and Proxy Services that enable greater accountability, the EWG incorporated Privacy/Proxy communication within its PBC principles. It also recommended Privacy/Proxy principles and a framework as input to the GNSO Privacy and Proxy Services Accreditation Issues Working Group.

To address the needs of individuals and groups who can demonstrate that they would be at risk if identified in registration data, the EWG recommends a Secure Protected Credential framework whereby those parties may anonymously apply for and receive domain names registered using secure credentials, aided by attestors and trusted third parties to provide a shield between at-risk entities and Registrars. The EWG recommends that ICANN facilitate the establishment of an independent trusted review board that will validate claims of at-risk organizations or individuals to approve (and when necessary, revoke) credentials.

Data Quality

The EWG recommends more robust validation of Registrant data than provided by either today's WHOIS system or enhancements that may be achieved through broad implementation of the 2013 RAA. Baseline improvements to data quality include the following.

- The provision of purpose-driven contacts by Registrants should lead to significant improvements for reachability of appropriate contacts for various purposes and provides an incentive for Registrants to provide accurate information for those roles.
- With gated access to more sensitive data elements, Registrants would have less incentive to supply inaccurate data, coupled with more accountability for ensuring data accuracy.

In addition, the EWG recommends two related but independent improvements:

- Standard validation of all gTLD registration data, using both periodic checks and validation at the time of collection, with an option to pre-validate blocks of contact data for reuse in multiple domain name registrations, as well as the ability for RDS users to see when data was last validated and to what level; and
- A pre-validated Contact Directory, conceptually separate from the Domain Name Directory, to promote the quality and re-usability of data elements used to contact domain name Registrants and people or organizations that can be designated by Registrants as PBCs for various purposes associated with a domain name registration, and to deter the fraudulent use of personal data.

Principles and processes detailing these recommendations can be found in Section V.

Implementation Models

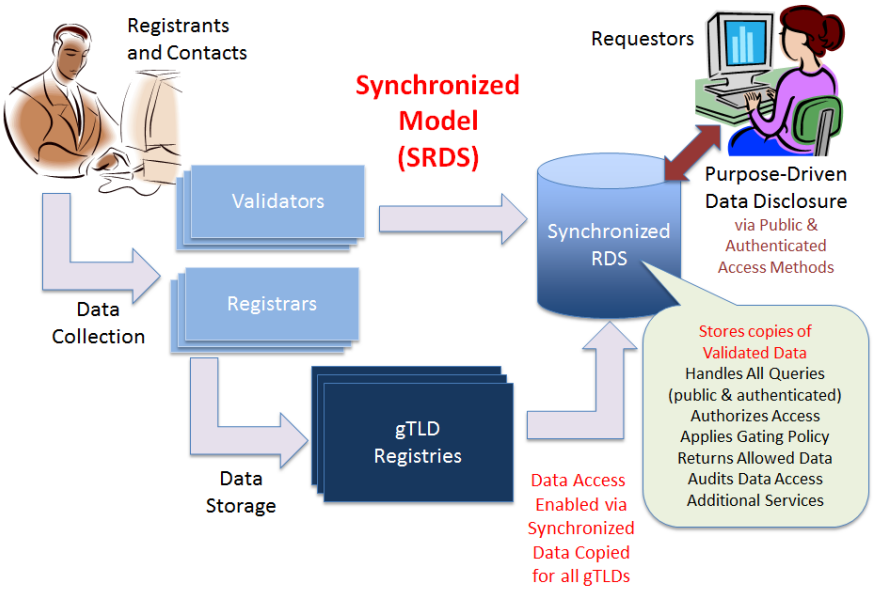
In considering how to put these principles and recommendations into practice, the EWG explored several alternative models in-depth. All models were evaluated using a set of multi-faceted criteria as identified in Annex F. After rigorous analysis, the EWG concluded the following.

- Today, Registrars or Registrar's Affiliates collect and store registration information from their own customers (Registrants). This process is inherently distributed. In addition to continuing to collect registration data from Registrants by Registrars or Affiliates, the EWG proposes collection of contact data by Validators.
- Multiple possible models exist for storing registration information across all gTLDs. The EWG identified several possible models and pinpointed two that it found to be most promising, and it recommends that one be chosen using evaluation criteria.

- To protect data subject privacy, a centralized interface must enable appropriate requestors to access registration information across all gTLDs, including unauthenticated public data access and authenticated gated data access.
- The RDS must use RDAP or EPP (as appropriate for each interface) as the underlying directory access protocol to obtain registration information from storage locations, wherever that may be.

The EWG developed and tested several alternative system models, detailed in Annex F, including models suggested by the ICANN community. These possible models differ in the way that registration information is copied to or queried through the RDS. The EWG closely examined each model to determine the impact of these differences. After comparing these possible models, the EWG found that, except for the current WHOIS, all are capable of satisfying the EWG's recommended RDS principles to some degree. Of these, the EWG focused on the two most promising models for further examination – the Federated Model and the Synchronized Model (formerly known as the "Aggregated Model").

To further inform its analysis, the EWG commissioned an Implementation Model Cost Analysis conducted by a neutral third party (IBM) to determine the requirements and potential costs of these two models. Based on the EWG's in-depth analysis, as well as IBM's Analysis Report, which found the Federated Model to be more costly to the entire RDS ecosystem, **the EWG ultimately recommended the Synchronized RDS (SRDS).**



Conclusion

Due to the extensive detail, complexity and length of the Final Report, this Executive Summary is not a comprehensive overview and readers are encouraged to refer to the body of this Final Report for additional information.

The EWG has delivered this Final Report to ICANN's CEO and Board, publicly posted it online, and will hold multiple public consultations at ICANN's June 2014 meeting in London. It will also conduct webinars and other opportunities to discuss the report and answer questions about it with the ICANN community. This Final Report is intended to serve as a foundation for the Board-requested GNSO Policy Development Process (PDP) for the provision of gTLD registration data and for contractual negotiations, as appropriate.

The EWG is confident that this Final Report fulfils the ICANN Board's directive to help redefine the purpose and provision of gTLD registration data, and will provide a solid foundation to help the ICANN community (through the GNSO) create a new global policy for gTLD directory services.

II. EWG Mandate, Purpose, and Outputs

a. Mandate

The Expert Working Group on gTLD Directory Services (EWG) was formed by ICANN's CEO, Fadi Chehadé, at the request of ICANN's Board, to help resolve the nearly decade-long deadlock within the ICANN community on how to replace the current WHOIS system. Several community reports and studies[4] published during this period point to deficiencies in the current system that calls for a solution.

The EWG's mandate is to re-examine and define the purpose of collecting and maintaining gTLD directory services, consider how to safeguard the data, and propose a next-generation solution that will better serve the needs of the global Internet community. The group started with a tabula rasa, exploring and questioning fundamental assumptions about the purposes, uses, collection, maintenance and provision of registration data. The EWG considered each stakeholder involved in gTLD directory services, examining their needs for accuracy, access, and privacy, and possible approaches to meet those needs more effectively.

b. Purpose

To help guide the EWG in its deliberations, the group developed a high-level statement of purpose from which to test its conclusions and recommendations, as follows:

> In support of ICANN's mission to coordinate the global Internet's system of unique identifiers, and to ensure the stable and secure operation of the Internet's unique identifier system, information about gTLD domain names is necessary to promote trust and confidence in the Internet for all stakeholders.
>
> Accordingly, it is desirable to design a system to support domain name registration and maintenance which:
>
> - Provides appropriate access to accurate, reliable, and uniform registration data
> - Protects the privacy of personal information
> - Enables a reliable mechanism for identifying, establishing and maintaining the ability to contact Registrants

[44] Refer to Annex B for a list of reports that document deficiencies in WHOIS.

- Supports a framework to address issues involving Registrants, including but not limited to: consumer protection, investigation of cybercrime, and intellectual property protection
- Provides an infrastructure to address appropriate law enforcement needs

c. Outputs

On 24 June 2013, the EWG published its Initial Report, Frequently Asked Questions, and an online questionnaire, and kicked off an extensive consultation process within the ICANN community on its initial recommendations. In its Initial Report, the EWG concluded that today's WHOIS model—giving every user the same anonymous public access to (often inaccurate) gTLD registration data—should be abandoned. Instead, the EWG recommended a paradigm shift whereby gTLD registration data is collected, validated and disclosed for permissible purposes only, with some data elements being accessible only to authenticated requestors that are then held accountable for appropriate use.

The EWG arrived at this recommendation after full consideration of past reports detailing WHOIS deficiencies and the many different stakeholders that use today's WHOIS system. For each identified user group, the EWG analyzed the purposes satisfied by registration data and the individual data elements needed to do so. Informed by this analysis, the EWG recommended principles and features to guide the creation of a next-generation registration directory service (RDS). To illustrate how these principles might be implemented, the EWG also considered several alternatives and proposed a model for collecting and disclosing accurate domain name registration data elements for permissible purposes.

On 11 November 2013, after careful consideration of all comments and feedback received from the ICANN community, the EWG published a Status Update Report, highlighting the EWG's thinking on many key issues. The Status Update Report also provided a great deal more detail on the analysis that lay behind the Initial Report, as requested by the community.

The EWG has engaged in a detailed analysis of the feedback received on both of these Reports, using the Community's extensive and diverse input to inform its on-going work on open areas and to test and refine its recommendations. Due to the complexity of the task at hand and the importance of basing any next-generation RDS on a solid understanding of the benefits and impacts that would likely result, the EWG conducted

research in five areas: existing ccTLD and commercial data validation practices, existing Privacy/Proxy service provider practices, exploration of organizations capable of accrediting RDS users, and analysis of RDS risks/benefits and costs. The results of this research, published in March 2014, were used to further refine the EWG's recommendations.

At this juncture, the EWG has carefully considered past work on WHOIS, existing and possible future users of gTLD registration data and their purposes, input from the many diverse stakeholders in today's WHOIS system, existing practices associated with proposed RDS improvements, and analysis of RDS risks, benefits, and costs. All of these inputs have informed the EWG's recommendations[5] for a next-generation system, detailed in this final report to the ICANN board and intended to serve as focused input to the policy development process.

[5] Throughout this report, EWG principles use the following terms, based on definitions given in RFC 2119:

- MUST: This word, or the terms "REQUIRED" or "SHALL," means that the definition is an absolute requirement of this report.
- MUST NOT: This phrase, or the phrase "SHALL NOT," means that the definition is an absolute prohibition of this report.
- SHOULD: This word, or the adjective "RECOMMENDED," means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED," means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

III. Users and Purposes

a. Methodology

The EWG was encouraged to take a "clean slate" approach in its efforts to define the next-generation of registration directory services, rather than proposing improvements to the current WHOIS system, which is widely regarded as inadequate. Consistent with the Board's directive, the EWG commenced its analysis by examining existing and potential purposes for collecting, storing, and providing gTLD registration data to a wide variety of users.

To accomplish this, EWG members drafted an extensive set of actual use cases involving the current WHOIS system, analysing each of them to identify (i) the users who want access to data, (ii) their rationale for needing such access, (iii) the data elements they need and (iv) the purposes served by such data. Cases were also used to identify all stakeholders involved in collecting, storing and providing registration data, helping the EWG understand existing and potential workflows and ways in which these users and their needs might be better satisfied by a next-generation RDS.

These use cases were not intended to be exhaustive, but rather representative of the many uses of the current WHOIS system, illustrating a wide variety of users, needs and workflows. An inventory of use cases considered by the EWG is provided Annex C.

The EWG considered the totality of these use cases and the lessons learned from them in order to derive a consolidated set of stakeholders and desirable purposes that must be accommodated by the RDS, as well a set of potential misuses that the system must attempt to deter (see the next section of this report.) Moreover, the EWG consulted reference materials from previous WHOIS-related activities, community inputs, and use cases to examine specific needs in each of the areas set forth in Figure 1 below.

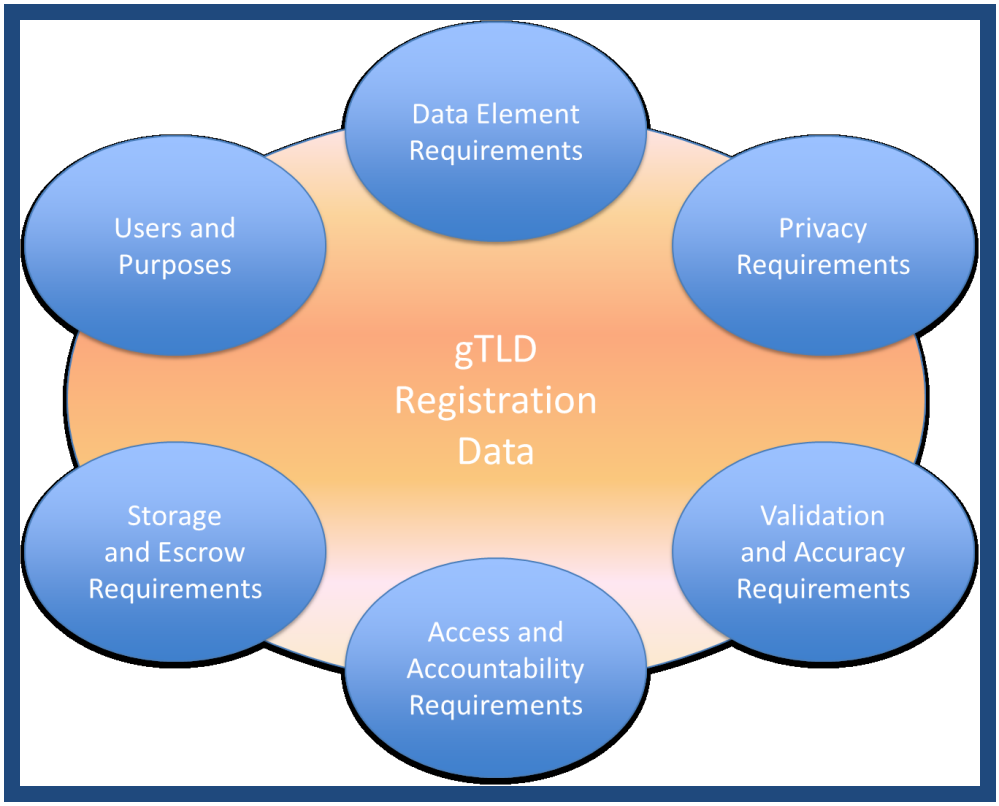


Figure 1: Needs Analysis

The EWG continued its work by analyzing these purposes and user needs to derive a minimum set of data elements needed for each purpose, risks related to making that data accessible, privacy law and policy implications of doing so, and additional questions explored in this report.

b. RDS Users and Purposes

Figure 2 below sets forth a non-exhaustive summary of users of the existing WHOIS system, including those with constructive or malicious purposes. Consistent with the EWG's mandate, all of these users were examined to identify existing and possible future workflows and the stakeholders and data involved in them.

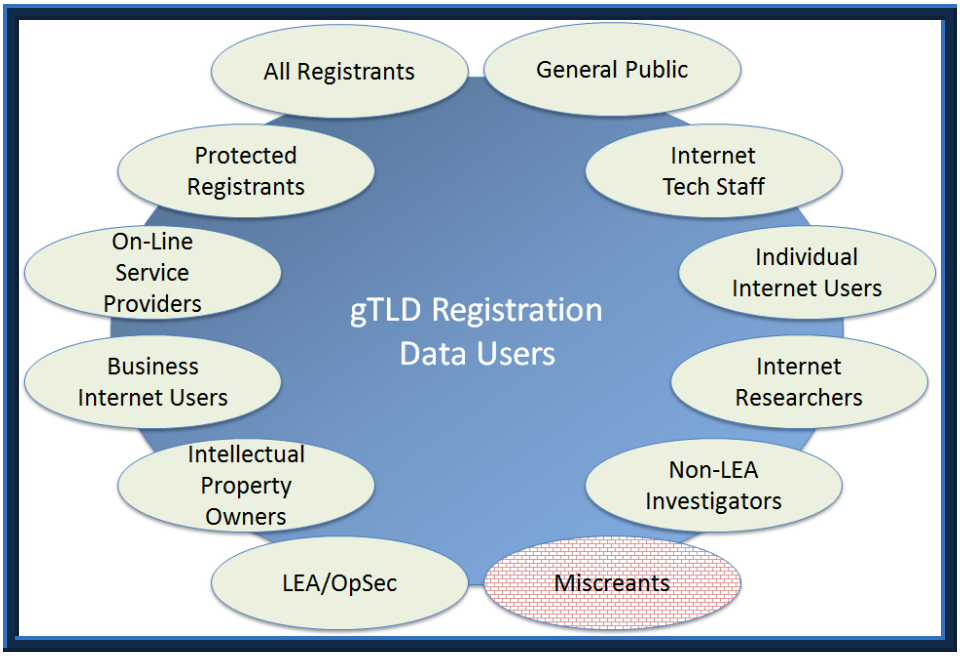


Figure 2: Users

In this report, the term "requestor" is used to refer generically to any of these users that wish to obtain gTLD registration data from the system. As further detailed in this report, the EWG recommends abandoning today's WHOIS model—giving every user the same anonymous public access to (too often inaccurate) gTLD registration data. Instead, the EWG recommends a paradigm shift whereby gTLD registration data is collected, validated and disclosed for permissible purposes only, with some data elements being accessible only to authenticated requestors that are then held accountable for appropriate use.

The EWG analyzed representative use cases to develop the following table, which summarizes the kinds of users who want access to gTLD registration data, the rationale for needing access, and the overall purposes served by that data. Further detail about each user, purpose, and associated data needs is provided in Section III(c), Purposes to be Accommodated or Prohibited, and Annex D.

User	Purpose	Example Use Cases	Rationale for registration data access
All Registrants (e.g., natural persons, legal persons, accredited Privacy/Proxy providers)	Domain Name Control	Domain Name Registration Account Creation	Enable registration of domain names by any kind of Registrant by creating a new account with a Registrar
		Domain Name Data Modification Monitoring	Detect accidental, uninformed or unauthorized modification of a domain name's registration data, either current or historical (using WhoWas)

User	Purpose	Example Use Cases	Rationale for registration data access
		Domain Name Portfolio Management	Facilitate update of all domain name registration data (e.g., designated contacts, addresses) to maintain a domain name portfolio
		Domain Name Transfer Initiation	Enable Registrant-initiated transfer of a domain name to another Registrar
		Domain Name Deletions	Enable deletion of an expired domain name
		Domain Name DNS Updates	Enable Registrant-initiated change of DNS for a domain name
		Domain Name Renewals	Enable renewal of a registered domain name by the domain name's Registrant
		Domain Name Contact Validation	Facilitate initial and on-going validation of registration data (e.g., designated contacts, addresses) by Registrant
Protected Registrants (e.g., customers of accredited Privacy/Proxy services that need to be contacted)	Personal Data Protection	Contact Privacy/Proxy Provider	Enable contact with accredited privacy or proxy providers offering registration services used by any Registrant seeking to minimize public access to personal names and addresses
		Contact Secure Credential Approver	Enable contact with accredited Secure Credential Approvers offering registration services used by individuals or groups under threat, using secure credentials relayed via trusted third party
Internet Technical Staff (e.g., DNS admins, mail admins, web admins, ISPs)	Technical Issue Resolution	Contact with Domain Name Technical Staff	Facilitate contact with technical staff (individual, role or entity) who can help resolve technical or operational issues with Domain Names (e.g., DNS resolution failures, email delivery issues, website functional issues)
Certification Authorities	Domain Name Certification	Domain Name Certification Issuance	Help a certification authority (CA) identify the Registrant of a domain name to be bound to an SSL/TLS certificate
Individual Internet Users (e.g., consumers)	Individual Internet Use	Real World Contact	Help consumers obtain non-Internet contact information for domain name Registrant (e.g., business address)
		Consumer Protection	Afford a lightweight mechanism for consumers to contact domain name Registrant-designated Business Contact (e.g., on-line retailer customer service) to resolve issues quickly, without LE/OpSec intervention

User	Purpose	Example Use Cases	Rationale for registration data access
Business Internet Users (e.g., brand holders, brokers, agents)	Business Domain Name Purchase or Sale	Domain Name Brokered Sale	Enable due diligence in connection with purchasing a domain name
		Domain Name Trademark Clearance	Enable identification of domain name Registrants to support trademark clearance (risk analysis) when establishing new brands
		Domain Name Acquisition	Facilitate acquisition of a domain name that was previously registered by enabling contact with Registrant
		Domain Name Purchase Inquiry	Enable determination of domain name availability and current Registrant and Admin Contact (if any)
		Domain Name Registration History	Provide domain name registration history to identify past Registrants and dates using WhoWas
		Domain Names for Specified Registrant	Enable determination of all domain names registered by a specified entity (Reverse Query) as part of merger/spinoff asset verification
Internet Researchers	Academic/ Public Interest DNS Research	Domain Name Registration History	Enable historical research about a domain name registration (WhoWas) during academic/public interest DNS research
		Domain Names for Specified Contact	Enable identification of all domains registered with a given name, address, name server, registration date, etc. (Reverse Query) during academic public interest DNS research
		Survey Domain Name Registrant or Designated Contact	Enable surveys of domain name Registrants or their designated contacts
Intellectual Property Owners (e.g., brand holders, trademark owners, IP owners)	Legal Actions	Domain Name User Contact	Enable contact with party using a domain name that is being investigated For TM/brand infringement or IP theft
		Combat Fraudulent Use of Registrant Data	Facilitate identification of and response to fraudulent use of legitimate data (e.g., address) for domain names belonging to another Registrant by using Reverse Query on identity-validated data.
		Domain Name Registration History	Enable historical research about a domain name registration (WhoWas) during IP infringement research

User	Purpose	Example Use Cases	Rationale for registration data access
		Domain Names for Specified Registrant	Enable identification of all domains registered with a given name or address (Reverse Query) during IP infringement research
Non-LEA Investigators (e.g., Tax Authorities, UDRP Providers, ICANN Compliance)	Regulatory and Contractual Enforcement	Online Tax Investigation	Facilitate by national, state, province or local tax authority identification of contacts for domain name engaged in on-line sales
		UDRP Proceedings	Let UDRP Providers confirm the correct respondent for a domain name, perform compliance checks, determine legal process requirements and protect against cyberflight
		RDS Ecosystem Contractual Compliance	Let ICANN audit and respond to complaints about non-compliance by contracted parties (e.g., data inaccuracy or unavailability, UDRP decision implementation, transfer complaints, data escrow and retention)
LEA/OpSec Investigators (e.g., law enforcement agencies, incident response teams)	Criminal Investigation & DNS Abuse Mitigation	Investigate Abusive Domain Name	Enable effective investigation and evidence gathering by LEA/OpSec personnel responding to an alleged maliciously-registered domain name, including examination of historical data
		Investigate Offline Criminal Activity	Enable effective investigation and evidence gathering by LEA/OpSec personnel responding to offline criminal activity by providing detailed registration data and/or searching for domain names registered to suspect (Reverse Query)
		Domain Name Reputation Services	Enable domain name white/black list analysis by reputation service providers
		Investigate Online Criminal Activity	Help victims or their legal counsel identify the domain name Registrant involved in potentially illegal activity to enable further investigation by LE/OpSec
		Abuse Contact for Compromised Domain Name	Assist in remediation of compromised domain names by helping LEA/OpSec personnel contact the Registrant or designated Abuse Contact

User	Purpose	Example Use Cases	Rationale for registration data access
General Public (e.g., bloggers, media, political activists)	DNS Transparency	Public Registration Data Access	Identify the organization "behind" a domain name, as commonly desired by a wide variety of Internet users not otherwise reflected in more specific use cases
Miscreants (e.g., those engaged in spam, DDoS, phishing, identity theft, domain hijack)	Malicious Internet Activities	Domain Name Hijack	Harvest domain name registration data to gain unlawful access to Registrant's account and hijacking that Registrant's domain name(s)
		Malicious Domain Name Registration	Use an existing/compromised domain name registration account to register new names to support criminal, fraudulent or abusive activities
		Registration Data Mining for Spam/Scams	Harvest domain name Registrant data for malicious use by spammers, scammers and other criminals (miscreants)

Table 1. RDS Users and Purposes

c. Purposes to be Accommodated or Prohibited

The EWG sought to prioritize the purposes enumerated above in order to focus use case development and narrow the spectrum of permissible purposes. However, it was difficult to establish a rationale for accommodating the needs of some users that access the current WHOIS system today but not others, so long as their purposes were not malicious. This finding led the EWG to recommend that all identified permissible purposes should be accommodated by the RDS *in some manner*, with the exception of known-malicious Internet activities that must be actively deterred. The EWG's recommended permissible purposes are therefore summarized below.

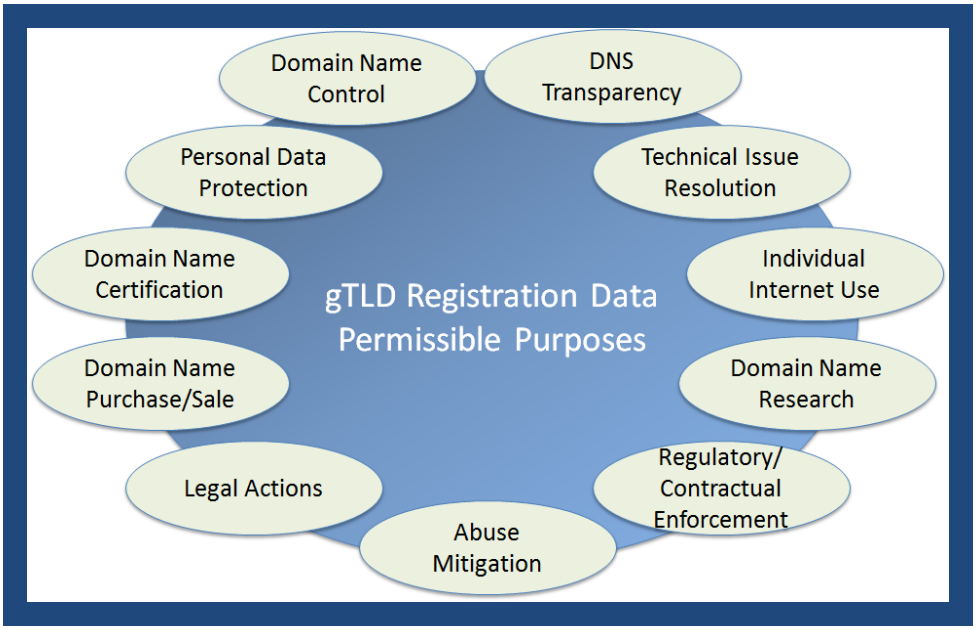


Figure 3: Permissible Purposes

It should be noted that, within each purpose, there are an infinite number of existing and possible future use cases. Although the EWG did not attempt to identify all possible use cases, it endeavoured to explore a representative sample in hopes of rigorously identifying kinds of users and their purposes in wanting access to gTLD registration data. However, the RDS must be designed with the ability to accommodate new users and permissible purposes that are likely to emerge over time.

As the EWG analyzed the use cases enumerated in Annex C, it became clear that many users have needs for similar data elements, but to satisfy different purposes. Some of these needs are well understood, for example:

- The ability to determine whether a domain name is registered
- The ability to determine the current status of a domain
- The ability to contact someone about the domain name

However, some needs are common and yet not readily fulfilled by the current WHOIS system in a consistent manner. Examples include:

- The ability to determine all domains registered by a given entity (commonly referred to as Reverse WHOIS)
- The ability to determine historical domain name registration information(commonly referred to as WhoWas)

The EWG took these common needs into consideration when developing the RDS recommendations detailed in this report. However, since it is likely that further common needs will be identified over time, any next-generation system must be designed with extensibility in mind. The EWG's currently-identified permissible purposes and associated registration data, contact, and query needs are further defined below.

Purpose	Definition
Domain Name Control	Tasks within the scope of this purpose include creating and managing and monitoring a Registrant's own domain name (DN), including creating the DN, updating information about the DN, transferring the DN, renewing the DN, deleting the DN, maintaining a DN portfolio, and detecting fraudulent use of the Registrant's own contact information. This implies that every Registrant must be an authenticated RDS user for this purpose, with the ability to access all public and gated information in the RDS about their DN, including designated contact data published in the RDS for this DN.
Personal Data Protection	Tasks within the scope of this purpose include identifying the accredited Privacy/Proxy Provider associated with a DN and reporting abuse, requesting reveal, or otherwise contacting the Provider. To accomplish these tasks, the user needs to reliably and easily contact the Privacy/Proxy Provider – for example, by following a Privacy/Proxy Provider PBC's Abuse_URL to a page that describes the provider's reveal process or allows the user to submit a reveal request form.
Technical Issue Resolution	Tasks within the scope of this purpose include working to resolve technical issues associated with domain name use, including email delivery issues, DNS resolution failures, and website functional issues. To accomplish these tasks, the user needs the ability to contact technical staff responsible for handling these issues. (Note: It might be useful to designate multiple points of contact to address various kinds of issues – for example, postmaster for email issues.)
Domain Name Certification	Tasks within the scope of this purpose include a Certification Authority (CA) issuing an X.509 certificate to a subject identified by a domain name. To accomplish this task, the user needs to confirm that the DN is registered to the certificate subject; doing so requires access to all public and gated data about the Registrant.
Individual Internet Use	Tasks within the scope of this purpose include identifying the organization using a domain name to instil consumer trust, or contacting that organization to raise a customer complaint to them or file a complaint about them. To accomplish these tasks, the user needs the name of the organization (preferably identity- validated) and its legal (postal) address, and may benefit from following a Contact URL to a page that describes the Organization and its customer service contacts or allows the user to submit a customer service inquiry.

Purpose	Definition
Business Domain Name Purchase or Sale	Tasks within the scope of this purpose include making purchase queries about a DN, acquiring a DN from another Registrant, and enabling due diligence research. To accomplish these tasks, the user needs access to the Registrant's Organization and email address, and in some cases additional gated data – for example, to perform a Reverse Query on the name of a Registrant or contact to determine other domain names with which they are associated.
Academic/Public Interest DNS Research	Tasks within the scope of this purpose include academic public interest research studies about domain names published in the RDS, including public information about the Registrant and designated contacts, the domain name's history and status, and DNs registered by a given Registrant (Reverse Query). To accomplish these tasks, the user needs the ability to access all public data in the RDS and in some cases might need access to gated data for use in anonymized, aggregated form.
Legal Actions	Tasks within the scope of this purpose include investigating possible fraudulent use of a Registrant's name or address by other domain names, investigating possible trademark infringement, contacting a Registrant/Licensee's legal representative prior to taking legal action and then taking a legal action if the concern is not satisfactorily addressed. To accomplish these tasks, the user needs the ability to contact the Registrant/Licensee's legal representative, without relay through an accredited Privacy/Proxy provider.
Regulatory and Contractual Enforcement	Tasks within the scope of this purpose include tax authority investigation of businesses with online presence, UDRP investigation, contractual compliance investigation, and registration data escrow audits. To accomplish this, the accredited user needs access to some gated Registrant contact and DN data elements, such as postal address and telephone number, as appropriate for the stated purpose. For example, WIPO may need access for UDRP resolution.
Criminal Investigation & DNS Abuse Mitigation	Tasks within the scope of this purpose include reporting abuse to someone who can investigate and address that abuse, or contacting entities associated with a domain name during an offline criminal investigation. To accomplish these tasks, the accredited user (e.g., law enforcement agent, first responder) needs to quickly and reliably reach the Abuse Contact responsible for the associated domain name – for example, by following a URL to an abuse reporting process description or incident report form.
DNS Transparency	Tasks within the scope of this purpose involve querying the registration data made public by Registrants to satisfy a wide variety of use cases around informing the general public. To accomplish these tasks, the user needs easy access to public data (and only public data) that can be supplied by the RDS. Registrants must be informed that their domain name registration public data may be used for this "catch all" purpose, and this purpose must be limited to public data (that is, this purpose does NOT allow access to gated data.)

Table 2. Purpose Definitions

The scope of registration data needed to fulfil these purposes is further summarized in the following table, including domain names involved, the kinds of data needed (Registrant data, contact data, domain name data), and additional queries needed.

Purpose	Query Scope	Contact(s) Needed	Registrant Data Needed	DN Data	Other Queries Needed
Domain Name Control	Own DN	All	Public+Gated	Yes	Reverse (Own Data) WhoWas (Own DN)
Personal Data Protection	PP DN*	PP	Public	Yes	None
Technical Issue Resolution	Any DN	Tech	Public	Yes	None
Domain Name Certification	Any DN	None	Public+Gated	Yes	None
Individual Internet Use	LP DN*	Business	Public	No	None
Business Domain Name Purchase or Sale	Any DN	Admin	Public+ Approved Gated	Yes	Reverse (Approved Data) WhoWas (Any DN)
Academic/Public Interest DNS Research	Any DN	All	Public+ Approved Gated	Yes	Reverse (Approved Data) WhoWas (Any DN)
Legal Actions	Any DN	Legal	Public+ Approved Gated	Yes	Reverse (Approved Data) WhoWas (Any DN)
Regulatory and Contractual Enforcement	Any DN	Legal	Public+Gated	Yes	Reverse (Any Data) WhoWas (Any DN)
Criminal Investigation & DNS Abuse Mitigation	Any DN	Abuse	Public+Gated	Yes	Reverse (Any Data) WhoWas (Any DN)
DNS Transparency	Any DN		Public	Yes	None

Table 3. Scope of Registration Data needed for each Purpose

In Table 3, "Approved Gated Data" could be defined by Terms of Service that accredited RDS Users can apply for, subject to defined policies which cover:

- Who qualifies for gated access
- Legitimate reasons for needing that data
- Limitations on use of that data
- Required oversight to ensure appropriate use

These purposes needing "Approved Gated Data" require further analysis, in consultation with those RDS User communities, to determine how such policies might reasonably be

defined, implemented, and enforced, balancing needs for accountability and privacy. However, the following examples are given to illustrate how this might work:

- **Academic/Public Interest DNS Research** might involve a researcher from a recognized university, engaged in a specified study of the DNS, having enumerated the gated data elements required and how they will be used, agreeing to publish results only in aggregated/anonymized form, subject to Independent Review Board (IRB) oversight. Having been approved to perform "Public Interest DNS Research," the accredited RDS User might be entitled to access certain gated Registrant data elements or query those data elements in a Reverse Query.
- **DN Purchase/Sale** investigation might involve a business user, engaged in a commercial transaction requiring due diligence about domain name assets held by a seller. With monitoring and oversight by an Accrediting Body (defined in Section IV(c), RDS User Accreditation), this user might attest that not only are they engaged in a domain name purchase, but that RDS data is needed to enable due diligence about seller "X" and results will be used only for this specific purpose. Having been approved to use the DNS to perform this kind of due diligence, the accredited RDS User might be entitled to use Reverse Queries to search for domain names with approved gated data tied to seller "X," as further detailed in Annex E.
- **Legal Action** investigation might involve a licensed attorney engaged in a trademark infringement investigation. With monitoring and oversight by an Accrediting Body (defined in Section IV(c), RDS User Accreditation), this user might attest that not only is he investigating a possible legal action, but that RDS data is being requested to enable investigation about subject "Y" and all data returned will be used only for this narrow purpose. Having been approved to use the DNS to perform this kind of trademark infringement investigation, the accredited RDS User might be entitled to use Reverse Queries to search for domain names with approved gated data tied to subject "Y," as further detailed in Annex E.

To illustrate the data involved in these purposes, the role of approved gated data, and the safeguards that might be put into place to hold users accountable and deter abuse, see Annex E, Illustrations of Gated & Unauthenticated Access.

This exploration of RDS Users and Permissible Purposes led the EWG to formulate the following foundational principles to enable purpose-based access to registration data:

No.	Permissible Purposes Principles
1.	ICANN must publish, in one place, a user-friendly policy describing the purpose and permissible uses of registration data, to clearly inform Registrants why this data is being collected and how it will be handled and used.
2.	There must be clearly defined permissible/impermissible uses of the RDS.
3.	The RDS must support defined permissible purposes, including uses that involve: • Identifying the Registrant and contacts designated for a given purpose; • Communicating with contacts designated for a given purpose; • Using data published by Registries about Domain Names; and • Searching portions of registration data required for a given purpose.
4.	The RDS must be designed with the ability to accommodate new users and permissible purposes that are likely to emerge over time. • An application process must be defined. • Applications must be reviewed against defined criteria • Applications that pass review must be evaluated and approved by a multistakeholder review board as determined by a policy development process • Approved applications must be added to the RDS privacy policy and scheduled for implementation periodically (e.g., quarterly, annually) as defined by policy Note: See Section VI Data Elements for process to add new data elements.
5.	All identified permissible purposes should be accommodated by the RDS *in some manner*, with the exception of known malicious Internet activities that must be actively deterred. The EWG's recommended permissible purposes are summarized in Table 1, RDS Users and Purposes, and Figure 3, Permissible Purposes.
6.	gTLD registration data should be collected, validated, and disclosed for permissible purposes only, with some data elements being accessible only to authenticated requestors that are then held accountable for appropriate use.
7.	Every Registrant must have the ability to access all public and gated information published in the RDS about their domain name, including designated contact data.

d. Stakeholders Involved in the RDS

The following table provides a representative summary of the various stakeholders involved in collecting, storing, disclosing and using gTLD registration data, mapped to associated purposes. Some stakeholders supply data (e.g., Registrants), while others collect/store data (e.g., Validators, Registrars, Registries) or disclose data (e.g., RDS Provider, accredited Privacy/Proxy Service providers). However, most stakeholders are parties involved in initiating data requests (e.g., brand owners, their agents) or parties identified, contacted or otherwise impacted by data disclosed (e.g., domain name Abuse Contacts). This summary is intended to illustrate the breadth of stakeholders most likely to be affected by the RDS. However, in any given transaction involving registration data, there may well be additional stakeholders not enumerated here.

Stakeholders	Purposes
Abuse Contact for Domain Name	Criminal Investigation & Abuse Mitigation
Acquiring Company	Business Domain Name Purchase or Sale
Acquiring Company's Agents/Attorneys	Business Domain Name Purchase or Sale
Address Validation Service	Domain Name Control
Agents of Registrant	Domain Name Control
Brand Holder	Regulatory/Contractual Enforcement
Brand Management Service Provider	Domain Name Control
Brand Owner	Business Domain Name Purchase or Sale
Certification Authority	Domain Name Certification
Complainant	Regulatory/Contractual Enforcement
Consumers purchasing goods from Websites	Individual Internet Use
Internet Users accessing Websites	Individual Internet Use
Domain Broker	Business Domain Name Purchase or Sale
Domain Buyer	Business Domain Name Purchase or Sale
Fraud Victim	Legal Actions
Fraud Victim's Agent	Legal Actions
Government Agency Personnel	Regulatory/Contractual Enforcement
ICANN Compliance	Regulatory/Contractual Enforcement
Independent Review Board (IRB)	Academic/Public Interest DNS Research
Internet Service Providers	Technical Issue Resolution Criminal Investigation & Abuse Mitigation
Investigator	Individual Internet Use
Law Enforcement Personnel	Criminal Investigation & Abuse Mitigation Legal Actions
Listed Privacy/Proxy Provider Contact	Personal Data Protection Domain Name Control Academic/Public Interest DNS Research
Listed Tech Contacts	Technical Issue Resolution Domain Name Control Academic/Public Interest DNS Research
Listed Admin Contacts	Regulatory/Contractual Enforcement Domain Name Purchase/Sale Domain Name Control Academic/Public Interest DNS Research
Listed Legal Contacts	Legal Actions

Listed Business Contacts	Regulatory/Contractual Enforcement Academic/Public Interest DNS Research Individual Internet Use Domain Name Control
Listed Abuse Contacts	Academic/Public Interest DNS Research Criminal Investigation & Abuse Mitigation Domain Name Control Academic/Public Interest DNS Research
Online Service Provider	Technical Issue Resolution
Op/Sec Service Providers	Criminal Investigation & Abuse Mitigation
Organization Sponsoring Study	Public Interest DNS Name Research
Person/Entity under investigation	Regulatory/Contractual Enforcement
Privacy/Proxy Service Customer	Business Domain Name Purchase or Sale Domain Name Control Technical Issue Resolution Regulatory/Contractual Enforcement Personal Data Protection
Privacy/Proxy Service Provider	Criminal Investigation & Abuse Mitigation Business Domain Name Purchase or Sale Domain Name Control Public Interest DNS Name Research Technical Issue Resolution Legal Actions Personal Data Protection Regulatory/Contractual Enforcement Technical Issue Resolution
RDS Provider	All Purposes
Registrant	All Purposes
Registrant's Legal Contact	Legal Actions Regulatory/Contractual Enforcement
Registrar	Business Domain Name Purchase or Sale Domain Name Control Public Interest DNS Name Research Individual Internet Use Legal Actions Personal Data Protection Regulatory/Contractual Enforcement Technical Issue Resolution Criminal Investigation & Abuse Mitigation
Registry	All Purposes
Reporter of Problem	Technical Issue Resolution
Researcher	Academic/Public Interest DNS Research
Reseller	DN Control Criminal Investigation & Abuse Mitigation
Resolver of Problem	Technical Issue Resolution
Target of Legal/Civil Action **Third Parties seeking Contact**	Individual Internet Use Legal Actions Personal Data Protection
Secure Credential Approver	Personal Data Protection
Secure Credential Recipient	Personal Data Protection
UDRP Panellists	Regulatory/Contractual Enforcement
UDRP Provider	Regulatory/Contractual Enforcement

Validator	All Purposes
Victim of Abuse	Criminal Investigation & Abuse Mitigation
Web Hosting Provider	Technical Issue Resolution

Table 4. Representative Summary of Stakeholders

e. Purpose-Based Contact Principles

The existence and use of Internet domain names within public zones creates potential external effects on third parties worldwide. From abusive behavior, to technical problems, to rights infringements and domain name issues large and small, there are myriad reasons a third party somewhere in the world may have a legitimate need to contact a person or organization associated with a particular domain name.

At the same time, Registrants of domain names may desire and be entitled (depending on their local jurisdiction) to privacy. They may not want their contact details made public. Further, Registrants are often not the best person or entity to solve whatever issue may be raised by a third party---for example, problems related to the DNS configuration of a domain name or responding to a trademark dispute. Therefore, providing Registrant information alone will likely be unsatisfactory for third parties looking to resolve issues associated with a domain name.

The diverse nature of potential issues will require differing responses – both in content and timeliness -- to situations that are often logically solved by different people and/or organizations associated with a particular domain. At the very least, however, any domain name must have one or more publicly published, accurate, and reachable contact that may respond to external queries and provide a point of reference for permissible purposes of external actors who are affected by the existence or operations of a domain name.

Timeliness of response may be a desired goal for policymaking for particular contact types. However, that goal has to be balanced against the burdens that response requirements could create on the entities fulfilling those roles. Gaming of the system, inappropriate requests or intentional overloading of contacts should not lead to any penalties for those contacts. It is desirable for requestors to have a process to escalate failed communication with a non-responsive contact for certain purposes (e.g., dealing with abuse issues, responding to UDRP filings). Failure to respond to such a process could potentially lead to suspension and/or deletion of that contact and potentially affected domain name(s) in a codified process. However, specific policy goals for response timeliness are beyond the scope of this report.

No.	Purpose-Based Contact Principles
8.	At least one Purpose-Based Contact (PBC) must be provided for every registered domain name which makes public the union of all mandatory data elements for all mandatory PBCs. This PBC must be syntactically accurate and operationally reachable to meet the needs of every codified permissible purpose.
9.	During domain name registration, the Registrant's Contact ID[6] must be used as the default PBC ID for each purpose. The Registrant must be informed of all permissible purposes and given an opportunity to publish other PBC IDs for each purpose, including replacing the Registrant's Contact ID for any or all purposes.
10.	A Purpose-Based Contact does not have to be the Registrant, and access to the Registrant's information may be highly gated as per other policies. Note that a PBC does not necessarily represent a person but rather a designated point of contact for various purposes.
11.	A domain name must not be activated (put into the global DNS) until a valid PBC ID is provided for every applicable purpose. If a PBC becomes invalid for its designated purpose, a process that provides the Registrant with the ability to specify a new valid contact must ensue, allowing reasonable notification and time for PBC ID update to occur. As per Principle #9 above, the Registrant's Contact ID must be used as the default PBC ID for each purpose. Failure to provide a valid PBC ID beyond that time could lead to suspension and/or deletion of the domain name in a codified process. (See Section V for Validation requirements.)
12.	PBC ID's can optionally be provided for every permissible purpose, with varying defined requirements for data elements that need to be collected and published for each type of PBC in order to fulfill the needs of associated permissible purposes.
13.	A process and policies must be developed enabling Registrant-designated contacts to opt-in/opt-out of having their Contact IDs published as PBC IDs for domain names, to support the rights of persons and entities to accept or reject responsibility for serving in specific roles for particular domain registrations.
14.	Any system for providing "Purpose-Based Contacts" must be flexible and allow for new purposes and contact types to be created and published in the RDS.

[6] Contact IDs are identifiers associated with blocks of contact data to enable retrieval and update, introduced in Section IV(a), Data Elements, and defined in Section V(d), Operational Framework for Contact IDs.

No.	Purpose-Based Contact Principles
	(See Section III(c) for further detail about adding new purposes.)

f. Purpose-Based Contact Roles and Responsibilities

As summarized in Figure 4 and detailed in Table 1, the EWG analyzed representative use cases to identify the kinds of users who want access to gTLD registration data and the permissible purposes currently served by that data. To deliver purpose-based access to registration data, all permissible purposes have been mapped to PBCs. For example:

- A "legal" contact can be designated to handle TM disputes or other legal claims regarding a domain name. To enable contact for associated purposes, this PBC just have a physical address capable of receiving legal notice, an active email address to receive inquiries, and a working phone or fax number to receive queries.
- An "abuse" contact can be designated to handle inquiries about abusive behavior emanating from a domain and manifesting in traffic or other highly time-sensitive malicious Internet activities. To enable contact for associated purposes, this PBC must have an email address capable of receiving and responding to valid complaints and an active phone number to receive inquiries. The PBC may also include Social Media and Instant Messaging addresses to facilitate real-time interaction, a physical address or fax number to receive queries, and a published URL that facilitates abuse reporting.

PBCs are also recommended to designate administrative, technical, accredited Privacy/Proxy Provider, and business contacts. A complete list of PBC types and responsibilities is provided in Table 5; see also Section IV, Data Collection Principle #20, for data element needs for every PBC type.

As shown in the following figure, the EWG recommends that the Registrant's own ID be used if more specific PBCs are not provided for a given domain name. For example, if a Legal Contact has not been specified for a given domain name, the Registrant should be informed that parties may need to contact them for this permissible purpose and be given an opportunity to designate a PBC to receive such requests for this domain name.

If the Registrant opts not to designate a PBC, such requests will be sent to the Registrant, using data required for this purpose associated with the Registrant's Contact ID. If the Registrant prefers to not make public those data elements, the domain name may be registered using an accredited Privacy/Proxy service. See Section IV for further discussion of Data Element principles and PBCs.

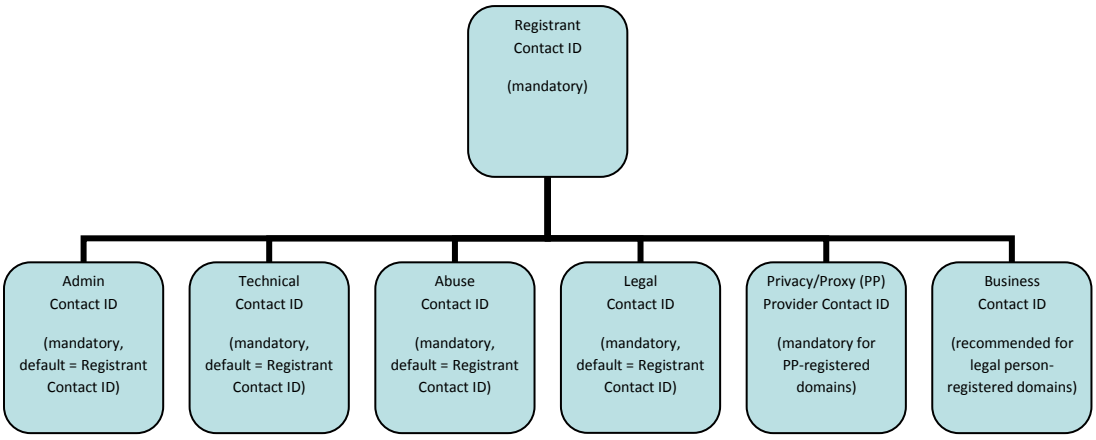


Figure 4. RDS Contact Types

All purposes/contacts must be codified by policymakers through a defined process for adding, changing, or deleting purposes.

This PBC approach preserves simplicity for Registrants with basic contact needs and offers additional granularity for Registrants with more extensive contact needs. To illustrate this concept, three different fictional but typical examples are given below:

1. A Registrant may explicitly designate their Registrant Contact ID as their domain name's only point of contact. In this case, RDS queries for every permissible purpose will return authorized public or gated data elements associated with the Registrant's Contact ID, as required for each purpose.

Example DN Record:

```
Registrant Contact ID = <reg>
Tech Contact ID = <reg>
Admin Contact ID = <reg>
Abuse Contact ID = <reg>
Legal Contact ID = <reg>
```

2. A Registrant using an accredited **Privacy** service (defined in Section VII) might designate several unique Contact IDs for their domain name, including a Privacy/Proxy Provider Contact ID (i.e., the Privacy service provider), a Tech Contact ID (e.g., hosting provider or ISP), and provider-supplied Admin, Abuse, and Legal Contact IDs. In this example, the designated Tech Contact is responsible for resolving all Technical Issues associated with the domain name, and accredited Privacy/Proxy Provider Contact is responsible for all privacy services associated with the domain name (including forwarding Admin, Abuse, and Legal Contact messages to the Registrant.)

Example DN Record:

```
Registrant Contact ID = <reg>
PP Contact ID = <pp>
Tech Contact ID = <isp>
Admin Contact ID = <reg@pp>
Abuse Contact ID = <reg@pp>
Legal Contact ID = <reg@pp>
```

3. A Registrant that has opted to self-identify as a legal person may supply many unique Contact IDs for a given domain name, including Legal, Abuse, and Business PBC IDs specifically associated with this domain name. In this example, RDS queries for each of these purposes will return data elements associated with a corresponding specialized PBC's ID, facilitating direct contact with the person or entity that has accepted responsibility for the designated role. This scenario may grow more common over time as larger organizations take advantage of this granularity to improve contactability and reduce miscommunication and redirection.

Example DN Record:

```
Registrant Contact ID = <reg>
Tech Contact ID = <isp>
Admin Contact ID = <admin@reg>
Abuse Contact ID = <abuse@reg>
Legal Contact ID = <legal@reg>
Business Contact ID = <cs@reg>
```

These examples are illustrated graphically in the following figure:

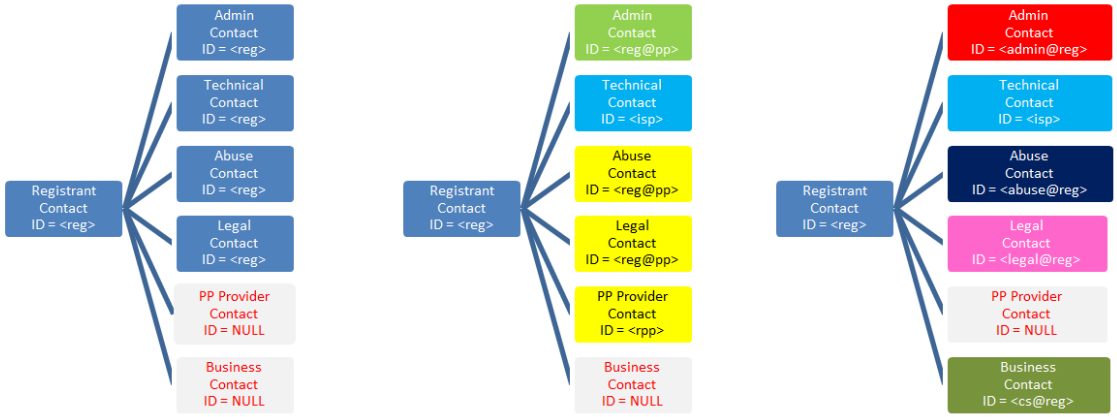


Figure 5. Example DN Registrations using Purpose-Based Contacts

Refer to Section IV for a list of recommended PBCs and to Annex D for a complete list of data elements associated with each permissible purpose and associated PBC.

PBC responsibilities include receiving requests about this domain name, evaluating those requests, and acknowledging the request and/or notifying the Registrant/Licensee, depending upon the contractual agreement between the Registrant and the PBC.

Potential responsibilities for each PBC can be summarized as follows:

PBC Type	Potential Responsibilities
Admin	Handling requests related to domain name acquisition and sale, such as purchase inquiries and domain name transfers.
Legal	Handling requests about this domain name from tax authorities, UDRP investigators, contractual compliance investigators, and legal representatives.
Technical	Handling requests about this domain name related to problems with website outages, DNS issues, mail delivery issues, etc.
Abuse	Handling DNS abuse reports about this domain name, including phishing, spam, and other harmful Internet activities.
Privacy Proxy	Handling requests for relay/reveal, fielding complaints about domain name abuse on behalf of the Registrant/Licensee, complying with LEA investigations into criminal activities.
Business	Handling consumer requests for information about a business and information for contacting the company for further information or to resolve customer complaints.

Table 5. Potential Responsibilities for each Purpose-Based Contact

For Future Consideration: There could be multiple PBCs specified for each type of PBC, allowing direct contact with specific individuals with critical responsibilities. For example, for a large Internet presence, it would be desirable to divide technical issues among the postmaster, the DNS operator, the webmaster, etc. The duties performed by such specialized contacts would be labelled in a field that would be published in public data to identify the specific purpose for the PBC as designated by the Registrant. This complexity is likely not warranted at this time, but should not be precluded in the future.

g. RDS Contact Use Authorization

As described above, domain name registrations must designate at least the minimum needed PBCs. All such contacts must be aware of and agree to fulfill the designated role(s) for each registered domain name. Principles associated with this concept further detailed below.

No.	Purpose-Based Contact Use Authorization Principles
15.	Each PBC's approval must be obtainable in a scalable, real-time or near real-time manner to avoid delaying domain name registrations or domain name updates.
16.	Policies and processes must prevent unauthorized use of PBCs.
17.	Either the PBC or the Registrant must be able to rescind approval at a later time. (See Section V, Validation for details)
18.	Registrants must be able to easily designate themselves as PBC's for their domain names without external/third party approval.

For example, a Registrant supplies a PBC Contact ID and a one-time use token that can be instantly and automatically verified by the Validator responsible for that Contact ID. Alternatively, an email or SMS verification system could be employed in a process to obtain contact authorization.

IV. Improving Accountability

The recommended RDS takes a clean slate approach, abandoning today's one-size-fits-all WHOIS in favor of purpose-driven access to validated data in hopes of improving privacy, accuracy and accountability.

The EWG believes that a gated access paradigm could increase accountability for all parties involved in the disclosure and use of gTLD domain name registration data. First, the RDS would log all access to gTLD registration data, including unauthenticated access to public data elements, and access restrictions to deter bulk harvesting. In addition, gated access to more sensitive data elements would only be available to requestors who applied for and were issued credentials for RDS query authentication. Finally, the RDS would audit both public and gated data access to minimize abuse and impose penalties and other remedies for inappropriate use. Different terms and conditions might be applied to different purposes. If requestors violate terms and conditions, penalties would apply.

Many ICANN community members have raised concerns about abandoning entirely anonymous public WHOIS in favor of the EWG's recommended gated access paradigm. Some suggested that all registration data should remain public to entirely anonymous requestors, while others suggested that little or no data should be public. Some supported the concept of accrediting users requesting access for permissible purposes, but sought additional detail on available data elements, accreditation processes, and how policies related to permissible purposes would be established and refined over

time. While there is no easy answer to satisfy these diverse views, this Section details the EWG's recommendations in these areas.

a. Data Element Principles

The EWG recommends the following principles to categorize data elements.

No.	Data Element Principles
19.	The RDS must accommodate purpose-driven disclosure of data elements. (See Section III for a list of permissible purposes and associated Purpose-Based Contacts (PBCs).)
20.	Not all data collected is to be public; disclosure must depend upon Requestor and Purpose.
21.	Public access to an identified minimum data set must be made available, including PBC data published expressly to facilitate communication for this purpose.
22.	Data Elements determined to be more sensitive (after conducting the risk & impact assessment) must be protected by gated access, based upon: • Identification of a permissible purpose • Disclosure of requestor/purpose • Auditing/Compliance to ensure that gated access is not abused
23.	Only the data elements permissible for the declared purpose must be disclosed (i.e., returned in responses or searched by Reverse and WhoWas queries).
24.	The only data elements that must be collected are those with at least one permissible purpose.
25.	Each data element must be associated with a set of permissible purposes. • An initial set of acceptable uses, permissible purposes, and data element needs are identified by this report (see Section III and Annex D). • Each permissible purpose must be associated with clearly-defined data element access and use policies. • As specified in Section III, an on-going review process must be defined to consider proposed new purposes and periodically update permissible purposes to reflect approved additions, mapping them to existing data elements. • A Policy Definition process must be defined to consider proposed new data elements and, when necessary, update defined data elements, mapping them to existing permissible purposes.

No.	Data Element Principles
26.	The list of minimum data elements to be collected, stored and disclosed must be based on known use cases (reflected in this document) and a risk assessment (to be completed prior to RDS implementation).
27.	All Registries and Validators must store the full set of data elements that they collect/provide to the RDS. (See also Section VII, Possible RDS Models.)

Step 1: Data Collection

Data must be collected before it can be selectively disclosed for permissible purposes. The following principles are recommended to guide collection at registration time:

No.	Data Collection Principles
28.	In support of the overarching legal principles given in Section VI, Registrars and Validators should afford domain name Registrants and Purpose-Based Contacts the opportunity, at the time of data collection, to consent to the use of their data for pre-disclosed permissible purposes, in accordance with the data protection laws of their jurisdiction. In formulating the policy, this principle must be addressed in the broader context of these overarching legal principles.[7]
29.	To meet basic domain control needs, it must be mandatory for Registries and Registrars to collect and Registrants to provide the following data elements when a domain name is registered: a. Domain Name b. DNS Servers c. Registrant Name d. Registrant Type Indicates the kind of entity identified by Registrant Name, for use in applying registration data requirements, as follows: **Undeclared** – Applies by default if none of the following options are selected and shall be treated by the RDS in a manner similar to natural person. **Privacy/Proxy Provider** – Must be selected for domain names registered using an accredited Privacy/Proxy Provider. When selected, a Contact ID of an accredited Privacy/Proxy Provider must also be supplied to enable relay/reveal request escalation to the PP PBC.

[7] There was near unanimous support for this text, with one EWG member dissenting.

No.	Data Collection Principles
	Legal Person – May be selected for domain names registered to entities that are NOT natural persons NOR proxy providers. When selected, a Contact ID of a designated Business PBC must also be supplied to facilitate consumer inquiries and complaints. (See note below this table.) **Natural Person** – May be selected for domain names registered to natural persons. When selected, neither Privacy/Proxy PBC nor Business PBC shall be defined, and Registrant Name and addresses shall be treated as personal information in compliance with Data Protection laws applicable to the data subject's jurisdiction. e. Registrant Contact ID A unique ID assigned to each Registrant Contact [Name+Address] during validation (refer to Section V for a more detailed definition of Contact ID and how it is created through a Validator and used for DN registration) f. Registrant Postal Address Includes the following data elements: Street, City, State/Province, Postal Code, Country (as applicable) g. Registrant Email Address h. Registrant Phone Includes the following data elements: Number, Extension (when applicable)
30.	a. To improve both Registrant privacy and contactability, Registrars must collect and Registrants must provide Purpose-Based Contacts (PBCs) for every registered domain name. b. Registrants may optionally designate Privacy/Proxy-supplied PBCs or authorized third party PBCs for specified permissible purposes (see Section III). c. To meet the communication needs associated with each permissible purpose, PBCs created through a Validator and subsequently associated with a domain name must satisfy the following minimum mandatory data element requirements: Tech Contact: Email Address Admin Contact: Organization, Email Address Legal Contact: Organization, Email Address, Phone, Postal Address Abuse Contact: Email Address, Telephone Number Business Contact[8]: Organization, Postal Address

[8] Contact is mandatory only if Registrant Type = Legal Person

No.	Data Collection Principles
	Privacy/Proxy Provider Contact[9]: Organization, Email Address, Contact_URL, Abuse_URL d. If a Registrant does not designate a PBC for each mandatory permissible purpose, the Registrant's own Contact ID must be used by the default for those PBCs. (Note that the Registrant can avoid this by using an accredited Privacy/Proxy service, or by designating PBCs.) When the Registrant's Contact ID is used as a PBC ID, collection and disclosure requirements on the Registrant's data may be increased to satisfy the above-stated PBC mandatory data element needs.
31.	To avoid collecting more data than necessary, all other Registrant-supplied data not enumerated in principles #29 or 30 above and used for at least *one* permissible purpose must be optionally collected at the Registrant's discretion. Validators, Registries and Registrars must allow for this data to be collected and stored if the Registrant so chooses.
32.	To maximize Internet stability, the following mandatory data elements must be provided by Registries and Registrars to the RDS: a. Registration Status b. Client Status (Set by Registrar) c. Server Status (Set by Registry) d. Registrar e. Registrar Jurisdiction f. Registry Jurisdiction g. Registration Agreement Language h. Creation Date i. Registrar Expiration Date j. Updated Date k. Registrar URL l. Registrar IANA Number m. Registrar Abuse Contact Phone Number n. Registrar Abuse Contact Email Address o. URL of Internic Complaint Site
33.	For TLD-specific data elements, the TLD Registry must establish and publish a data collection policy (consistent with these over-arching principles) and be responsible

[9] Contact is mandatory only if Registrant Type = Privacy Proxy Provider

No.	Data Collection Principles
	for any validation of those TLD-specific data elements.
34.	Validators, Registries and Registrars may collect, store, or disclose additional data elements for internal use that is never shared with the RDS.[10]

Note: After considerable discussion, the EWG has not recommended adding **Domain Name Purpose** as a data element. Instead, the EWG has recommended principles to accomplish associated goals and an explicit **Business PBC** recommended for publication by Registrants that self-identify as **Legal Persons** engaged in commercial activity. This might result in many commercial Internet users more uniformly publishing data elements to boost consumer confidence, while acknowledging that Registrants are ultimately self-selecting this classification and it would be nearly impossible to globally enforce rigorous compliance around Domain Name Purpose = Commercial vs. Non-Commercial.

Step 2: Data Disclosure

After data is collected, it can be selectively disclosed for permissible purposes. The following principles are recommended to guide disclosure when queries are received:

No.	Data Disclosure Principles
35.	To maximize Registrant privacy, Registrant-supplied data must be gated by default, except where there is a compelling need for public access that exceeds resulting risk. • Registrants can opt into making any gated Registrant-supplied data public with informed consent.
36.	To maximize Internet stability, all Registry or Registrar-supplied registration data must be always public, except where doing so results in unacceptable risk. • Registrants can opt into making any public Registry/Registrar-supplied data gated, except as noted below to enable basic domain control.
37.	To maximize reachability, all PBCs must be public by default.

[10] Examples include the IP address used by the customer at the time of registration, a link to request generation of an EPP transfer key for a domain name, and payment data associated with the customer's account. Internal use data is not standardized by the RDS but rather privately defined by Registries and Registrars.

No.	Data Disclosure Principles
	• Contact Holders[11] can opt into making any PBC data element gated, except those required to satisfy the designated purpose (further detailed in Table 5).
38.	To meet basic domain control needs, the following Registrant-supplied data, which is mandatory to collect and low-risk to disclose, must be included in the minimum public data set: a. Domain Name b. DNS Servers c. Registrant Type d. Registrant Contact ID (further defined in Section V) e. Registrant Email Address f. Tech Contact ID g. Admin Contact ID h. Legal Contact ID i. Abuse Contact ID j. Privacy/Proxy Provider Contact ID (mandatory only if Registrant Type = Privacy/Proxy Provider) k. Business Contact ID (mandatory only if Registrant Type = Legal Person)
39.	To balance simplicity and reachability, if a Registrant does not supply a mandatory PBC, the Registrant must be informed that his or her Contact ID will be used as that PBC, and Registrant data elements will be published as the domain name's Tech Contact, Admin Contact, Legal Contact, and Abuse Contact. The Registrant can avoid this disclosure by specifying one or more third party PBCs or by using an accredited Privacy/Proxy service (in which case those addresses will be supplied by the service provider).
40.	For TLD-specific data elements, the TLD Registry must establish and publish a data disclosure policy (consistent with these over-arching principles) and be responsible for identifying permissible purposes for any gated TLD-specific data elements.

[11] Per Section III(g), RDS Contact Use Authorization, designated PBCs must authorize use of a Contact ID within a given domain name registration. In doing so, Contact Holders also agree to public/gated use of their data for that purpose. However, if a pre-validated PBC does not contain the mandatory/public data elements to meet a given purpose, that PBC cannot be designated for that purpose in a domain name registration.

Resulting Data Element Classifications

Based on these principles, the following table details the resulting classification for each RDS data element recommended by the EWG, using the following notation:

- Whether each element is (M)andatory or (O)ptional to Collect. This means:

  [1] For data collected from Registrants,
  (M)andatory means data must be requested by Registrars/Validators and provided by Registrants, while
  (O)ptional means data must be requested by the Registrar/Validator but may or may not be provided at the Registrant' s discretion, as applicable.

  [2] For data collected from Purpose-Based Contact Holders,
  (M)andatory means data must be requested by Registrars/Validators and provided by Contact Holders, while
  (O)ptional means data must be requested by the Registrar/Validator but may or may not be provided at the Contact Holder's discretion, as applicable, and

  (R)ecommended means data must be requested by the Registrar/Validator but may or may not be provided at the Contact Holder' s discretion, as applicable, to reflect both "Best" and "Good" practice recommendations[12]

  [3] For data provided by Registries and Registrars to the RDS,
  (M)andatory means data must be provided by the Registry/Registrar, while
  (O)ptional means data may or may not be provided, as applicable.

- Whether each element is (P)ublic [accessible to everyone, with or without authentication] or (G)ated [accessible to authenticated users only, for permissible purposes only], and whether Registrants can change that default disclosure setting (Y/N). This means:

[12] Recommended best practices for publishing various PBC data elements are based on EWG members' operational experience. The mandatory elements represent a minimum operational requirement to carry out those purposes. However, in practice, if a communication method exists for a given purpose (e.g., a web form for reporting issues, alternative email to reach technical staff) then that alternative method is highly useful and often preferred for handling issues. This will vary across PBCs – for example, a postal address is more useful for Legal or Business Contact purposes and largely useless to quickly resolve Abuse or Technical Contact purposes. Thus, the EWG has made specific recommendations for data elements in each type of PBC.

[4] For data collected from Registrants,

P / N means any data collected must be public and cannot be hidden,

P / Y means any data collected is public by default but can be hidden by Registrant,

G / Y means any data collected is gated by default but can be made public by Registrant, with informed consent.

[5] For data provided by Registries and Registrars to the RDS,

P / N means any data provided must be public and cannot be hidden, while

G / N would mean any data provided must be gated; no data elements fall into this category.

[6] For data collected from Purpose-Based Contact Holders,

P / N means any data collected must be public and cannot be hidden,

P / Y means any data collected is public by default but can be hidden by Contact Holder

Note that whether gated data elements are accessible to a given user depends on permissible purposes. When a Registrant opts to make a gated-by-default element public, it becomes accessible to everyone. When a Registrant opts to make a public-by-default element gated, access is then limited to permissible purposes.

REGISTRY/REGISTRAR PROVIDED DATA	Collection M or O	Disclosure Default P or G	Disclosure Can Be Changed?	Notes See [3] Collection Definition and [5] Disclosure Definition
Registration Status	**M**	**P**	**N**	
DNSSEC Delegation	O	**P**	**N**	
Client Status (Registrar)	**M**	**P**	**N**	Contains all values applicable to domain name at Registrar level: DeleteProhibited, RenewProhibited, TransferProhibited
Server Status (Registry)	**M**	**P**	**N**	Not in RAA, similar to above, but at Registry level
Registrar	**M**	**P**	**N**	
Reseller	O	**P**	**N**	
Registrar Jurisdiction	**M**	**P**	**N**	Not in RAA
Registry Jurisdiction	**M**	**P**	**N**	Not in RAA
Reg Agreement Language	**M**	**P**	**N**	Not in RAA
Creation Date	**M**	**P**	**N**	
Original Registration Date	O	**P**	**N**	Not in RAA
Registrar Expiration Date	**M**	**P**	**N**	
Updated Date	**M**	**P**	**N**	
Registrar URL	**M**	**P**	**N**	
Registrar IANA Number	**M**	**P**	**N**	
Registrar Abuse Contact Email Address	**M**	**P**	**N**	
Registrar Abuse Contact Phone Number	**M**	**P**	**N**	
URL of Internic Complaint Site	**M**	**P**	**N**	

REGISTRANT DATA collected from Registrant	Collection M or O	Disclosure Default P or G	Disclosure Can Be Changed?	Notes See [1] Collection Definition and [4] Disclosure Definition
Domain Name	**M**	**P**	**N**	
DNS Servers	**M**	**P**	**N**	
Registrant Name	**M**	G	Y	
Registrant Type	**M**	**P**	**N**	
Registrant Contact ID	**M**	**P**	**N**	Replaces Registry Registrant ID, issued by Validator in RDS
Registrant Contact Validation Status	**M**	**P**	**N**	New, Supplied by Validator
Registrant Contact Last Validated Timestamp	**M**	**P**	**N**	New, Supplied by Validator
Registrant Organization	O	**P**	Y	Collected when Registrant Type = Legal Person or Proxy Provider
Registrant Company Identifier (e.g., Trading Name, D-U-N-S)	O	**P**	Y	Real-world identifiers issued to businesses by sources such as Dunn and Bradstreet Collected when Registrant Type = Legal Person Not in RAA
Registrant Street Address	**M**	G	Y	
Registrant City	**M**	G	Y	
Registrant State/Province	O	G	Y	Per the 2013 RAA, all "State/Province" elements collected when applicable
Registrant Postal Code	O	G	Y	Per the 2013 RAA, all "Postal Code" elements collected when applicable
Registrant Country	**M**	G	Y	
Registrant Phone + Ext	**M**	G	Y	Extension collected if applicable
Registrant Alt Phone + Ext	O	G	Y	New option, not in RAA
Registrant Email Address	**M**	**P**	**N**	
Registrant Alt Email	O	**P**	Y	New option, not in RAA
Registrant Fax + Ext	O	G	Y	Per the 2013 RAA, all "Fax" and “Fax Ext” elements collected

				when applicable
Registrant SMS	O	G	Y	New option, not in RAA
Registrant IM	O	G	Y	New option, not in RAA
Registrant Social Media	O	G	Y	New option, not in RAA
Registrant Alt Social Media	O	G	Y	New option, not in RAA
Registrant Contact_URL	O	G	Y	New option, not in RAA
Registrant Abuse_URL	O	G	Y	New option, not in RAA

PURPOSE-BASED CONTACTS Admin Contact	**Collection M/R/O**	**Disclosure Default P or G**	**Disclosure Can Be Changed?**	**Notes** See [2] Collection Definition and [6] Disclosure Definition
Purposes: DN Purchase/Sale, Domain Name Control, DNS Research				
Admin Contact ID	**M**	**P**	**N**	
PBC ID	**M**	**P**	**N**	Not in RAA
PBC Validation Status	**M**	**P**	**N**	New, Supplied by Validator
PBC Last Validated Timestamp	**M**	**P**	**N**	New, Supplied by Validator
PBC Name	**M**	**P**	**N**	
PBC Organization	**M**	**P**	**N**	
PBC Street Address	R	**P**	Y	
PBC City	R	**P**	Y	
PBC State/Province	O	**P**	Y	
PBC Postal Code	O	**P**	Y	
PBC Country	**M**	**P**	**N**	
PBC Phone + Ext	O	**P**	Y	
PBC Alt Phone + Ext	O	**P**	Y	Not in RAA
PBC Email Address	**M**	**P**	**N**	
PBC Alt Email Address	O	**P**	Y	Not in RAA
PBC Fax + Ext	O	**P**	Y	
PBC SMS	O	**P**	Y	Not in RAA
PBC IM	O	**P**	Y	Not in RAA
PBC Social Media	O	**P**	Y	Not in RAA
PBC Alt Social Media	O	**P**	Y	Not in RAA
PBC Contact_URL	O	**P**	Y	Not in RAA
PBC Abuse_URL	O	**P**	Y	Not in RAA

PURPOSE-BASED CONTACTS Legal Contact	Collection M/R/O	Disclosure Default P or G	Disclosure Can Be Changed?	Notes See [2] Collection Definition and [6] Disclosure Definition
Purposes: Legal Actions, Regulatory/Contractual, Domain Name Control, DNS Research				
Legal Contact ID	**M**	**P**	**N**	Not in RAA
PBC ID	**M**	**P**	**N**	Not in RAA
PBC Validation Status	**M**	**P**	**N**	New, Supplied by Validator
PBC Last Validated Timestamp	**M**	**P**	**N**	New, Supplied by Validator
PBC Name	**M**	**P**	**N**	
PBC Organization	**M**	**P**	**N**	
PBC Street Address	**M**	**P**	**N**	
PBC City	**M**	**P**	**N**	
PBC State/Province	O	**P**	Y	
PBC Postal Code	O	**P**	Y	
PBC Country	**M**	**P**	**N**	
PBC Phone + Ext	**M**	**P**	**N**	
PBC Alt Phone + Ext	O	**P**	Y	Not in RAA
PBC Email Address	**M**	**P**	**N**	
PBC Alt Email Address	O	**P**	Y	Not in RAA
PBC Fax + Ext	**R**	**P**	**Y**	
PBC SMS	O	**P**	Y	Not in RAA
PBC IM	O	**P**	Y	Not in RAA
PBC Social Media	O	**P**	Y	Not in RAA
PBC Alt Social Media	O	**P**	Y	Not in RAA
PBC Contact_URL	O	**P**	Y	Not in RAA
PBC Abuse_URL	O	**P**	Y	Not in RAA

PURPOSE-BASED CONTACTS Technical Contact	Collection M/R/O	Disclosure Default P or G	Disclosure Can Be Changed?	Notes See [2] Collection Definition and [6] Disclosure Definition
Purposes: Technical Issue Resolution, Domain Name Control, DNS Research				
Technical Contact ID	**M**	**P**	**N**	
PBC ID	**M**	**P**	**N**	Not in RAA
PBC Validation Status	**M**	**P**	**N**	New, Supplied by Validator
PBC Last Validated Timestamp	**M**	**P**	**N**	New, Supplied by Validator
PBC Name	R	**P**	Y	
PBC Organization	R	**P**	Y	
PBC Street Address	R	**P**	Y	
PBC City	R	**P**	Y	
PBC State/Province	O	**P**	Y	
PBC Postal Code	O	**P**	Y	
PBC Country	**M**	**P**	**N**	
PBC Phone + Ext	**R**	**P**	Y	
PBC Alt Phone + Ext	**R**	**P**	Y	Not in RAA
PBC Email Address	**M**	**P**	**N**	
PBC Alt Email Address	**R**	**P**	Y	Not in RAA
PBC Fax + Ext	O	**P**	Y	
PBC SMS	**R**	**P**	Y	Not in RAA
PBC IM	**R**	**P**	Y	Not in RAA
PBC Social Media	O	**P**	Y	Not in RAA
PBC Alt Social Media	O	**P**	Y	Not in RAA
PBC Contact_URL	**R**	**P**	Y	Not in RAA
PBC Abuse_URL	O	**P**	Y	Not in RAA

PURPOSE-BASED CONTACTS Abuse Contact	Collection M/R/O	Disclosure Default P or G	Disclosure Can Be Changed?	Notes See [2] Collection Definition and [6] Disclosure Definition
Purpose: Abuse Mitigation, Domain Name Control , DNS Research				
Abuse Contact ID	**M**	**P**	**N**	Not in RAA
PBC ID	**M**	**P**	**N**	Not in RAA
PBC Validation Status	**M**	**P**	**N**	New, Supplied by Validator
PBC Last Validated Timestamp	**M**	**P**	**N**	New, Supplied by Validator
PBC Name	R	**P**	Y	
PBC Organization	R	**P**	Y	
PBC Street Address	R	**P**	Y	
PBC City	R	**P**	Y	
PBC State/Province	O	**P**	Y	
PBC Postal Code	O	**P**	Y	
PBC Country	**M**	**P**	**N**	
PBC Phone + Ext	**M**	**P**	**N**	
PBC Alt Phone + Ext	O	**P**	Y	Not in RAA
PBC Email Address	**M**	**P**	**N**	
PBC Alt Email Address	O	**P**	Y	Not in RAA
PBC Fax + Ext	O	**P**	Y	
PBC SMS	O	**P**	Y	Not in RAA
PBC IM	**R**	**P**	Y	Not in RAA
PBC Social Media	**R**	**P**	Y	Not in RAA
PBC Alt Social Media	O	**P**	Y	Not in RAA
PBC Contact_URL	**R**	**P**	Y	Not in RAA
PBC Abuse_URL	**R**	**P**	**Y**	Not in RAA

PURPOSE-BASED CONTACTS Privacy/Proxy (PP) Provider Contact	Collection M/R/O	Disclosure Default P or G	Disclosure Can Be Changed?	Notes See [2] Collection Definition and [6] Disclosure Definition
Purposes: Personal Data Protection, Domain Name Control, DNS Research				
PP Contact ID	**M**	**P**	**N**	Not in RAA
PBC ID	**M**	**P**	**N**	Not in RAA
PBC Validation Status	**M**	**P**	**N**	New, Supplied by Validator
PBC Last Validated Timestamp	**M**	**P**	**N**	New, Supplied by Validator
PBC Name	**M**	**P**	**N**	
PBC Organization	**M**	**P**	**N**	
PBC Street Address	**M**	**P**	**N**	
PBC City	**M**	**P**	**N**	
PBC State/Province	O	**P**	Y	
PBC Postal Code	O	**P**	Y	
PBC Country	**M**	**P**	**N**	
PBC Phone + Ext	**M**	**P**	**N**	
PBC Alt Phone + Ext	O	**P**	Y	Not in RAA
PBC Email Address	**M**	**P**	**N**	
PBC Alt Email Address	O	**P**	Y	Not in RAA
PBC Fax + Ext	O	**P**	Y	
PBC SMS	O	**P**	Y	Not in RAA
PBC IM	O	**P**	Y	Not in RAA
PBC Social Media	O	**P**	Y	Not in RAA
PBC Alt Social Media	O	**P**	Y	Not in RAA
PBC Contact_URL	**M**	**P**	**N**	Not in RAA
PBC Abuse_URL	**M**	**P**	**N**	Not in RAA

PURPOSE-BASED CONTACTS Business Contact	Collection M/R/O	Disclosure Default P or G	Disclosure Can Be Changed?	Notes See [2] Collection Definition and [6] Disclosure Definition
Purposes: Individual Internet Use, Domain Name Control, DNS Research				
Business Contact ID	**M**	**P**	**N**	Not in RAA
PBC ID	**M**	**P**	**N**	Not in RAA
PBC Validation Status	**M**	**P**	**N**	New, Supplied by Validator
PBC Last Validated Timestamp	**M**	**P**	**N**	New, Supplied by Validator
PBC Name	**M**	**P**	**N**	
PBC Organization	**M**	**P**	**N**	
PBC Street Address	**M**	**P**	**N**	
PBC City	**M**	**P**	**N**	
PBC State/Province	O	**P**	Y	
PBC Postal Code	O	**P**	Y	
PBC Country	**M**	**P**	**N**	
PBC Phone + Ext	R	**P**	Y	
PBC Alt Phone + Ext	O	**P**	Y	Not in RAA
PBC Email Address	R	**P**	Y	
PBC Alt Email Address	O	**P**	Y	Not in RAA
PBC Fax + Ext	O	**P**	Y	
PBC SMS	O	**P**	Y	Not in RAA
PBC IM	O	**P**	Y	Not in RAA
PBC Social Media	O	**P**	Y	Not in RAA
PBC Alt Social Media	O	**P**	Y	Not in RAA
PBC Contact_URL	**R**	**P**	**Y**	Not in RAA
PBC Abuse_URL	O	**P**	Y	Not in RAA

The EWG also reiterates its recommendation to perform a widely scoped risk/impact analysis to confirm that these principle-based classifications do in fact result in appropriate collection and disclosure of data for defined purposes.

Alignment with 2013 RAA and New Data Elements

To facilitate transition and understanding, EWG-recommended data element names have been aligned with those identified in the 2013 RAA where possible (e.g., DNSSEC Delegation, RDS Expiration Date). However, data element names used in the 2013 RAA for contact data elements are not sufficient to reflect the EWG's proposal for Purpose-Based Contacts (see Section III). To cover this, the EWG applied the following mappings:

When RDS Admin Contact ID refers to a PBC,
RDS PBC Name = RAA Admin Contact Name
RDS PBC Organization = RAA Admin Contact Organization
and so forth for other RAA Admin Contact data elements

When RDS Technical Contact ID refers to a PBC,
RDS PBC Name = RAA Tech Contact Name
RDS PBC Organization = RAA Tech Contact Organization
and so forth for other RAA Tech Contact data elements

Note: The EWG recommends that the RDS portal make the definitions for every PBC type readily accessible to RDS users (for example, using hover-over pop-up definitions) to clearly indicate that PBCs are published to handle inquiries for permissible purposes, and that a point of contact must be designated to cover those purposes. Registrants may opt to receive inquiries themselves (designate the Registrant ID as the PBC), engage an accredited Privacy/Proxy provider to receive those inquires (engage a PP to supply those data elements – usually forwarding addresses or the provider's addresses), or designate a specific entity to receive those inquiries (e.g., a service provider, hosting provider, legal agent, customer service desk).

All data elements are as defined in the 2013 RAA, with the following additions:

Registrar and Registry Jurisdiction: The legal jurisdiction in which the Registrar or Registry operates, as indicated in their signed agreement with ICANN.

Registration Agreement Language: The language in which the Registrar's contract with the Registrant is written.

Original Registration Date: The date on which this domain name was first registered.[13]

Client Status, Server Status: Expanding upon 2013 RAA client status values, these data elements contain the Registrar (client) and Registry (server) status values currently applied to this domain name: DeleteProhibited, RenewProhibited, TransferProhibited.

Registrant Company Identifier: The UK trading number, D-U-N-S number, or other unique real-world company identifier assigned to the Registrant by a public business directory. This enables searching for a company outside the RDS.

[13] This is different than the creation date since the creation date picks up the latest time that the domain name was registered; it is possible that the domain name was previously registered and subsequently deleted multiple times. The Original Registration Date denotes the first date that the domain name was ever registered.

Registrant Contact ID: A unique handle assigned to a pre-validated block of contact data identified as this domain name's Registrant. Refer to Section V for a more detailed definition of Contact ID and how it is created and used. This ID enables reuse and maintenance of contact data within the RDS. Note that when Registrant Type = Privacy/Proxy, the Registrant Contact ID will reflect the unique identifier assigned to that accredited Privacy/Proxy Provider.

Registrant/PBC Contact Validation Status, Registrant/PBC Contact Last Validated Timestamp: The highest level of validation achieved and the date that is was most-recently validated, as further defined in Section V.

Registrant/PBC SMS, IM, Social Media: New contact methods that may optionally be used to reach the Registrant or PBC via SMS, instant messaging, or another alternative social media communication vector.

Registrant/PBC Alt Email, Alt Phone, Alt Social Media: New alternative addresses that may optionally be used to reach the Registrant or PBC when the primary address fails. These new data elements are intended to address common needs such as resolving tech issues when the domain name itself is down and enabling faster contact via mobile phone or social media.

Registrant/PBC Contact_URL, Abuse_URL: New data elements that optionally lead to web pages where contact or abuse reporting instructions, policies, or forms may be placed to facilitate more productive communication.

PBC Contact ID: A unique handle assigned to a pre-validated block of contact data identified as a PBC for this domain name, in the role indicated by the Contact Role. Registrant Contact ID and PBC Contact ID may or may not refer to the same contact.

Note: Transition and compliance challenges associated with these new data elements must be considered prior to any RDS implementation.

b. Principles for Unauthenticated and Gated Data Access

The EWG recommends that a new approach be taken for registration data access, abandoning entirely anonymous access by everyone to everything in favor of a new paradigm that combines public access to some data with gated access to other data. Principles that reflect this recommendation follow.

No.	Data Access Principles
41.	A minimum set of data elements, at least in line with the most stringent privacy regime, must be accessible by unauthenticated RDS users.

No.	Data Access Principles
42.	Multiple levels of authenticated data access must be supported, consistent with stated permissible purposes.
43.	RDS user access credentials must be tied to an auditable accreditation process, as further defined in Section IV(c), RDS User Accreditation.
44.	Access must be non-discriminatory (i.e., the process must create a level playing field for all requestors, within the same purpose).
45.	To deter misuse and promote accountability: • All data element access must be based on a stated purpose; • Access to gated data elements must be limited to authenticated requestors that assert a permissible purpose; and • Requestors must be able to apply for and receive credentials for use in future authenticated data access queries.
46.	Some type of accreditation must be applied to requestors of gated access: • When accredited Requestors query data, their purpose must be stated every time a request is made. • Different terms and conditions may be applied to different purposes. • If accredited requestors violate terms and conditions, penalties must apply.
47.	To raise the standard of gTLD registration data protection, all RDS queries/responses must make use of commonly-available message encryption and authentication measures to protect the confidentiality and integrity of data in transit.
48.	To meet the needs of authenticated RDS users with permissible purposes, the RDS must provide a Reverse Query service that searches public and gated data elements for a specified value and returns a list of all domain names that reference that value.
49.	To meet the needs of authenticated RDS users with permissible purposes, the RDS must provide a WhoWas service that returns historical snapshots of public and gated data elements for specified domain names, limited to the historical data available to the RDS.

No.	Data Access Principles
50.	The RDS must support innovative services that make use of RDS data elements, as follows. • Third parties must be able to provide existing and future innovative services – including Reverse Queries and WhoWas – using public data elements and held to terms and conditions of RDS data use. • In the event that third parties offer innovative services involving gated data elements, those third parties must be accredited and held to terms and conditions of RDS data use.
51.	All disclosures of gated data elements must occur through defined RDS access methods (including those described above). The entire RDS data set for all gTLDs (or the entire Registry data set for a single gTLD) must not be exported in bulk form for uncontrolled access.
52.	Disclosures may occur through interactive display and other RDS access methods. • To make data easier to find and access in a consistent manner, a central point of access (e.g., web portal) must be offered. • Secure access to public data must be available to all requestors through an unauthenticated query method (at minimum, via secure website). • Secure access to gated data must be supported through secure web and other access methods and formats (e.g., RDAP xml responses, SMS, email), based on authenticated requestor and purpose. • Requestors must be able to obtain authoritative data from the RDS in real-time when needed. • The RDS must accommodate automation for large-scale lookups for various use cases and permissible purposes.
53.	To be truly global, the RDS must accommodate the display of registration data in multiple languages, scripts and character sets, including Internationalized domain names (IDNs).
54.	The RDS should support all future GNSO-defined transliteration policies for gTLDs.

No.	Data Access Principles
55.	The RDS should enable collection and display of registration data elements in local languages.

Illustration of Public Data Access

As depicted in the following figure, public data elements can still be requested from the RDS by anyone, with or without authentication. Refer to Annex E for more detailed illustration of data elements returned to an unauthenticated public data query.

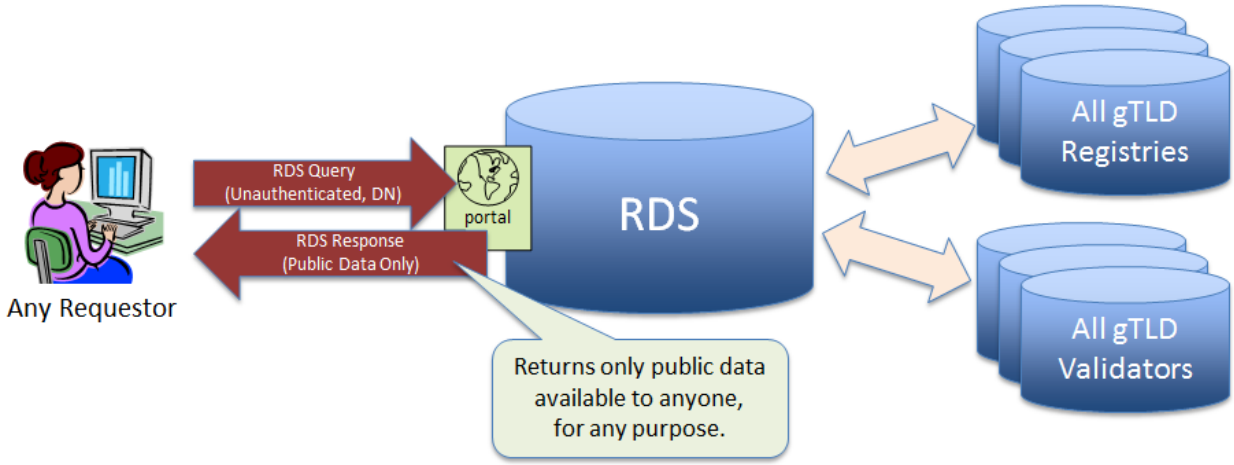


Figure 6. Unauthenticated Public Registration Data Access via RDS

Annex I also contains flow charts and an example use case to illustrate the steps involved in accessing the relevant data elements.

Illustration of Gated Data Access

As depicted in the following figure, gated data elements can also be requested via the RDS. To do so, requestors must first be accredited. Thereafter, requestors may submit authenticated queries requesting data elements for a stated purpose. Refer to Annex E for more detailed illustration of data elements returned to an authenticated gated data query.

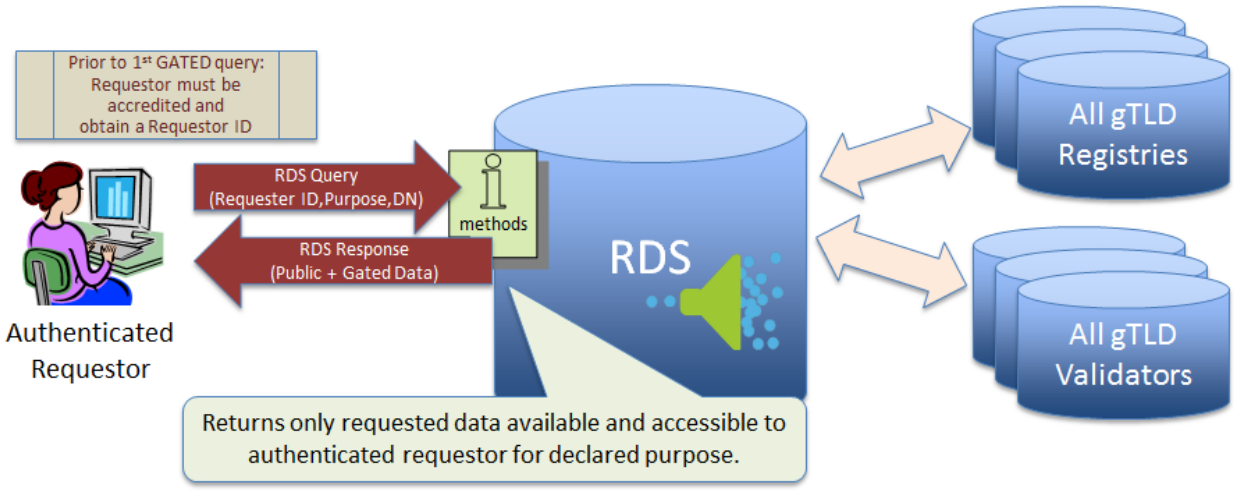


Figure 7. Gated Registration Data Access via RDS

Technical Protocols and Access Methods

The EWG examined whether the technical protocols deployed in today's domain registration system (such as EPP[14]), and under development in the IETF (such as by the WEIRDs working group), could support the design features recommended by the EWG. The WEIRDs group is close to finalizing a new standard referred to as the Registration Data Access Protocol (RDAP). Adopting these protocols in the EWG's recommended model may result in lower transition costs for each of the affected parties.

The EWG analyzed whether EPP could support each data element included in its recommended RDS, and whether RDAP could support the principles for access credentials recommended by the EWG. The EWG's analysis suggests that both EPP and RDAP can be used by the RDS, no matter which of the alternative models is chosen. However, doing so may require a few extensions, additions, or use of RDAP "remarks." A detailed assessment of each of these protocols is included in Annex G.

c. RDS User Accreditation Principles

As noted in Section III Purposes, some purposes require access to all gated elements or an approved subset of gated data elements. As noted in Section IV(b), Principle #46, any purpose requiring access to gated data requires user accreditation. However, user accreditation does not imply unlimited access to gated data. All access must be purpose-based, returning only data elements permitted for the stated purpose.

[14] See EPP: Standard 69, RFCs 5730 - 5734

The EWG recommends that, for each RDS User community identified in Section III desiring access to gated data for permissible purposes, community experts should be consulted to confirm EWG-identified registration data purposes, the data elements that must be accessible for that purpose, and possible RDS User Accreditors.

Many organizations are likely to enter into contracts with ICANN to serve as RDS User Accreditors. While all RDS User Accreditors must be guided by a common set of principles, differing implementations are likely for each RDS User community. For example:

Scenario #1: Accrediting Body separate from Accreditation Operator, where the Body approves Users, but a third party Operator manages accredited User access to the RDS

For an RDS User community such as Trademark Holders, an industry organization might take responsibility for accrediting its own members desiring access to gated data for permissible purposes. This Accrediting Body may play no role in managing user accounts or authenticating access requests sent to the RDS. Rather, the Accrediting Body establishes membership rules, terms of service, and application and enforcement processes, etc., for a given RDS User community. The Accrediting Body may then contract with a third party Accreditation Operator to create and manage RDS User accounts, issue RDS access credentials, authenticate RDS access requests, and provide first-level abuse handling, including temporary account suspension. The Accreditation Operator simply implements and enforces the RDS access rules established by the Accrediting Body for a given community; any account suspension appeals or other disputes would be escalated to the Accrediting Body.

Scenario #2: Accrediting Body combined with Accreditation Operator, passing authenticated RDS access requests to the RDS

For an RDS User community such as OpSec, an industry organization might take responsibility for accrediting its own members via an (approved) accreditation process that it already uses to grant users access to other systems. In this example, the organization serves as both the Accrediting Body and the Accreditation Operator, leveraging an existing system already used by its own members to authenticate and then pass along gated access requests for permissible purposes to the RDS. Here the RDS user is responsible for compliance with terms and conditions, and the industry organization must establish a process for dealing with access abuses, suspensions, etc., applied to a specific user's RDS accesses.

Scenario #3: Accrediting Body combined with Accreditation Operator, proxying access requests to the RDS on behalf of its members (i.e., the Interpol model)

For an RDS User community such as Law Enforcement, a recognized, trusted organization might take responsibility for accrediting its own members via an (approved) accreditation that it already uses to grant users access to other systems. In this example, the organization serves as both the Accrediting Body and the Accreditation Operator, leveraging an existing system already used by its own members to authenticate and then proxy gated access requests for permissible purposes to the RDS. Here, the organization is considered the RDS User and accepts responsibility for the actions of its members with regard to proxied requests and complying with terms and conditions. While the RDS may not be aware of specific user activities, the organization must establish a process for dealing with access abuses, suspensions, etc., in a way that allows the organization to audit specific user accesses and detect abuses.

To enable accredited RDS user access to gated data elements for permissible purposes, the EWG recommends the following RDS User Accreditation principles.

No.	RDS User Accreditation Principles
56.	Non-accredited, unauthenticated access to non-gated (i.e., public) data must be possible in real-time.
57.	Accreditation of RDS Users for access to RDS data does not have to happen in real-time for all use cases and/or requesters.
58.	The RDS must only apply the minimum "accreditation scheme" necessary to provide RDS User access to gated data elements for the stated purpose.[15]
59.	There must be no requirement to "pre-approve" or provide credentials to every potential user of the RDS. A request and fulfilment process can be created for each "type" of accredited RDS User (i.e., RDS User community).
60.	Accreditation for RDS users seeking access to data for permissible purposes could be granted in three ways. • None (i.e., unauthenticated access to public data only, as above). • Self-accreditation by the person/entity requesting the data, such as a system where the user simply states who they are, the data they are requesting and why, and then is granted access to that level of data. For example, this might apply to Registrants needing access to their own domain name's data for Domain Name Control purposes, where

[15] For example, this accreditation does not need to require multi-factor, sworn statements, or need to serve as a be-all-and-end-all system to get most types of data.

No.	RDS User Accreditation Principles
	their self-attestation is tied to the actual registration of a domain name, qualifying them for credentials to access that information in the RDS. • Accreditation by some trusted third party (i.e., RDS User Accreditor, see principle #64 below).
61.	Whenever possible, any third party RDS accreditation process should leverage existing accreditation processes within each RDS user community identified in Section III as one that would need credentialing.
62.	These third party accreditation processes must be vetted by an authority responsible for implementing and enforcing RDS User Accreditation policy (for example, ICANN, a multistakeholder panel) and reviewed on a periodic basis.
63.	Any organization serving as an RDS User Accreditor must have a signed agreement with ICANN and/or the RDS Provider to offer such accreditation processes under agreed-upon guidelines, and establish a framework to allow for due process, accountability, security, fair access, and adherence to applicable law.
64.	Accreditors may take on one or both of the following responsibilities. • An RDS User Accrediting Body may define and manage a user community, including establishing criteria for membership, setting credentialing requirements, and defining and enforcing its own terms and conditions of membership. • An RDS Users Accreditation Operator may offer a platform used by Accrediting Bodies, providing functions such as user account creation, credential issuance, suspension and revocation, lifecycle user account management, and associated processes such as dispute handling and ToC enforcement. A given Accreditor can, but is not required to, take on both responsibilities.
65.	Accreditors that wish to participate in handling RDS requests for data on behalf of their members may do so in two ways: • An Accreditor may provide proxied access to the RDS via their own authentication system and accept full responsibility for compliant usage. Although the Accreditor will be held accountable in the event of abuse, requests proxied through Accreditors in this manner must be authenticated in a way that enables auditing and abuse complaint resolution pertaining to an individual user's access. • An Accreditor may provide access to the RDS via their own authentication system, but simply relay authenticated requests to the

No.	RDS User Accreditation Principles
	RDS. Requests forwarded through the Accreditor in this manner must uniquely identify the RDS user, who is responsible for compliant usage and will be held directly accountable in the event of abuse.
66.	As defined in Section IV(b), Principle #50, the RDS must provide real-time access to credentialed requestors via multiple methods. Requests may be authenticated by the appropriate Accreditation Operator, and RDS access credentials issued during accreditation must be suitable for use with all defined access methods.[16]
67.	Best practices may be defined for credential management; Accreditors must be expected to adhere to best practices.
68.	The RDS must require individual credentials for authenticated access.
69.	Authenticated RDS access must not be transitive (i.e., an authenticated RDS user shall not share gated data with others outside of its accreditation).
70.	A process for responsible revelation of gated data to further the original purpose it was requested for must be created and enforced. (For example, enabling an IP Owner investigating trademark infringement to file a UDRP complaint, allowing an OpSec user investigating possible criminal activity to notify law enforcement.)
71.	An organization seeking access to RDS data could apply for RDS User accreditation and have all people using the RDS in their organization covered by that one accreditation.[17] Each such organization is responsible for managing accredited access within its own organization. Misuse of the system by members of an accredited RDS User organization would lead to sanctions against the organization as a whole.
72.	A single RDS user playing different roles may have multiple credentials in order to access different types of data for different purposes. However, it is highly desirable from a usability perspective to provide a single credential per RDS User that could be used for multiple purposes, as long as each purpose was stated per access as defined in Section IV(b).
73.	Audits and data analytics must be used to identify abuse of the system and access credentials.

[16] Authentication interfaces must be defined during implementation. For example, for some credential methods the RDS might use a standard framework such as the Security Assertion Markup Language (SAML) to enable authentication by the Accreditation Operator that issued that credential.

[17] It is up to the organization to ensure the integrity of any issued credentials for accessing the RDS.

No.	RDS User Accreditation Principles
74.	An appeals process must be defined to allow RDS users to refute abuse allegations when seeking to reactive/reinstate RDS access credentials.
75.	Every Registrant must receive a credential to be able to examine their own contact data as stored by the RDS in relation to domain names that are registered to them. (See Section III, Domain Name Control purpose.)
76.	A process for adding additional RDS User Accreditors that either supplement current processes or offer new, innovative ways to provide user accreditation for approved purposes of the RDS must be established. Such RDS User Accreditors must meet the minimum requirements as described in the principles enumerated here.

d. Summary of Accountability Key Benefits

Incorporating accredited access to gated data elements is an integral part of the next-generation RDS will improve accountability by requiring those who access more sensitive data to identify themselves and state their purpose for needing data. Specifically, benefits that would result from adopting the EWG's recommended data element and access principles include the following.

- Establishing a purpose-driven data collection and disclosure paradigm to promote accountability for entities that use registration data for permissible purposes.
- Providing a supporting framework to comply with data protection laws in various jurisdictions.
- Establishing a method to provide accountability for people accessing data for varied purposes. This further supports data protection/privacy requirements in various jurisdictions and ensures a balance of accountability between those being required to provide accurate data and those that use it for approved purposes. This addresses a fundamental inequity with the current WHOIS system where data requestors have no accountability for their access and use of contact data.
- Providing Registrants and contacts with a clearer understanding of the purposes for which registration data is collected and greater discretionary control over which personal information is public or gated.
- Meeting universal needs for registration data with a basic public data set, while also reducing data that is public by default and authenticating those who access gated data.

- Increasing data accuracy, due to protection of sensitive data elements from public disclosure, leading to more likely sharing of more accurate data by Registrants and PBCs. With the exception of miscreant use, when data is protected from general publication, data subjects will often provide more accurate information in order to receive the benefits of providing it, since a fundamental perceived risk is mitigated.
- Improving overall communication resiliency and efficiency for RDS Users and Registrants by incorporating new optional data elements to facilitate contact via new or alternative communication methods.
- Supporting Reverse and WhoWas Queries through a central portal to enable searches across all gTLD registrations, by accredited RDS Users for permissible purposes only.
- Enabling enhanced access capabilities to improve overall efficiency of the "system."
- Providing access, both unauthenticated to public data and via credentialed for gated data, to eliminate the hodgepodge of access capabilities, service levels, and formats in today's gTLD WHOIS responses, and allowing for easy implementation of automated RDS Queries via a single standard.
- Providing quality service and accountable access, allowing retirement of various anti-abuse measures distributed throughout the ecosystem.

To achieve these benefits, educating RDS users about permissible purposes and appropriate uses of data retrieved from the RDS will be paramount. Finding Accreditors willing to take on responsibility for approving RDS access by their community members may be challenging. Initially, there may be user confusion in identifying the appropriate Accreditor, especially for users who interact with the RDS for several purposes. Automated RDS Queries will also require updating tools. However, these initial investments necessary to establish purpose-driven access will lay a strong foundation for holding RDS users accountable for responsible use of registration data.

V. Improving Data Quality

The EWG recommends more robust validation of Registrant data than provided by either today's WHOIS system or enhancements that may be achieved through broad implementation of the 2013 RAA. First, the provision of PBCs by Registrants should lead to significant improvements in reachability of appropriate contacts for various purposes and creates an incentive for Registrants to provide accurate information for those roles. Second, gated access to more sensitive data elements would reduce Registrant incentive to supply inaccurate data and increase Registrant accountability for data accuracy.

To accomplish these goals, the EWG recommends two related but independent improvements:

- The RDS must apply standard validation to all gTLD registration data. In addition to periodic checks, validation would occur at the time of collection, with an option to pre-validate blocks of contact data for reuse in multiple domain name registrations.
- The RDS ecosystem must include a pre-validated Contact Directory, conceptually separate from the Domain Name Directory, to promote the quality and reusability of data elements used to contact domain name Registrants and people or organizations that can be designated by Registrants as PBCs for various purposes associated with a domain name registration, and to deter the fraudulent use of personal data.

Principles and processes detailing these recommendations are detailed below. For maximum benefit, the EWG recommends both improvements, but notes that creating a Contact Directory is possible without heightened validation and vice versa.

a. Data Accuracy and Validation Principles

Pre-validation of Registrant or other contact information is desired to:

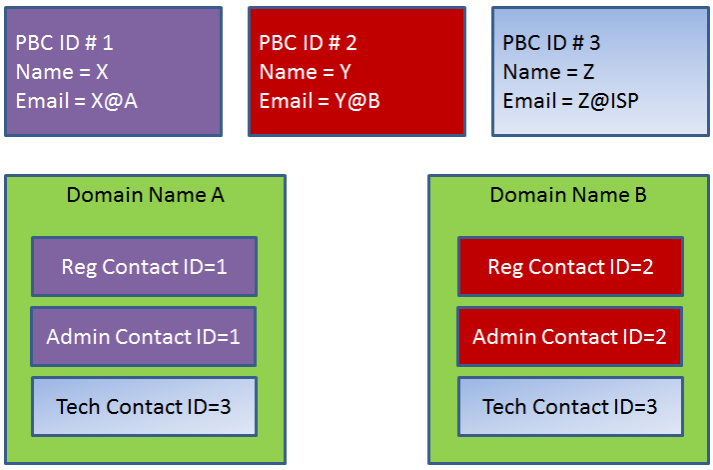
- Increase accuracy of contact information by utilizing pre-validation to check data prior to use for a new domain name and to promote consistent data across all registrations (reduces error and fraud);
- Avoid the need to validate Registrant or other PBC contact data each time a Registrant registers a new domain name by performing validation once and then reusing that block of contact data for several domain registrations (simplifies the process and reduces work requirements); and
- Avoid delay in the processing of a domain registration, since validation has to take place at the time of registration.

Many service providers, legal representatives, and other third parties are often the primary contact points for several roles (e.g. technical, billing, abuse, legal process) on domains registered by a wide variety of Registrants (often hundreds to hundreds of thousands of domains.)

To allow for much greater accuracy across such a diverse space and ease-of-use for such contacts, it is desirable to provide mechanisms to allow easy use of such contacts by multiple Registrants; for example, a web hosting company providing their NOC's unique ID for "technical" and "abuse" contacts for domains controlled by their customers.

Further, when such an entity needs to update their contact information to reflect a new address/phone number or a merger/acquisition, it should be easy to update that information in one place and have that reflected to all domains associated with that contact data set (as designated by a unique identifier).

The following figure illustrates a paradigm in which Purpose-Based Contacts (PBCs) might be created, associated with unique identifiers (PBC IDs), and then reused in multiple domain name registrations. As detailed in Section III, PBCs do not necessarily represent individual persons, but rather published points of contact expressly created by Contact Holders and intended to enable communication for DNS-related purposes.



Updates made to PBC ID # 3
automatically reflected in Registration Data for
Domain Names A and B

No.	Principles for Contact IDs and Associated Data
77.	Contact management must be feasible separately from domain management, allowing contact portability and accountability separate from domain names and controlled by the actual individuals or entities listed under such contacts.
78.	Contacts must be managed using Validators who manage contact databases, implement validation regimes, and maintain information on the level of validity for the contact and its data elements (accessible through the RDS).[18]
79.	Domain registrations may be associated with Contact IDs designated by their Registrants and approved by such designated contacts for various purposes

[18] NOTE: Registrars can and are presumed likely to become accredited Validators in order to provide validation services for contacts associated with domain names they register.

No.	Principles for Contact IDs and Associated Data
	associated with a domain name.
80.	Such contacts must contain valid mandatory data elements. Policies and oversight will be needed to manage these processes to ensure that Contact IDs are not used without contact's authorization and meet minimum standards.
81.	Change management and authorization of use of contact information is controlled by the Contact Holder and affects all domains associated to a contact. Processes and policies to ensure accurate, authentic, and timely implementation of desired changes without burdening PBCs or Registrants must be developed to support this new paradigm.
82.	Each individual block of contact data must have a Contact ID which uniquely identifies both the Validator and the Contact Holder to enable retrieval and update of associated contact data. This Contact ID must be published in any public display of RDS data.

b. Pre-validation Process

To address these needs, the following pre-validation process is recommended:

a) Each applicant submits contact data through a Validator of his or her choice (e.g. Registrar, Registry, accredited third party contact management provider).

b) Syntactic and operational validation (per SAC-058) is carried out by the Validator.

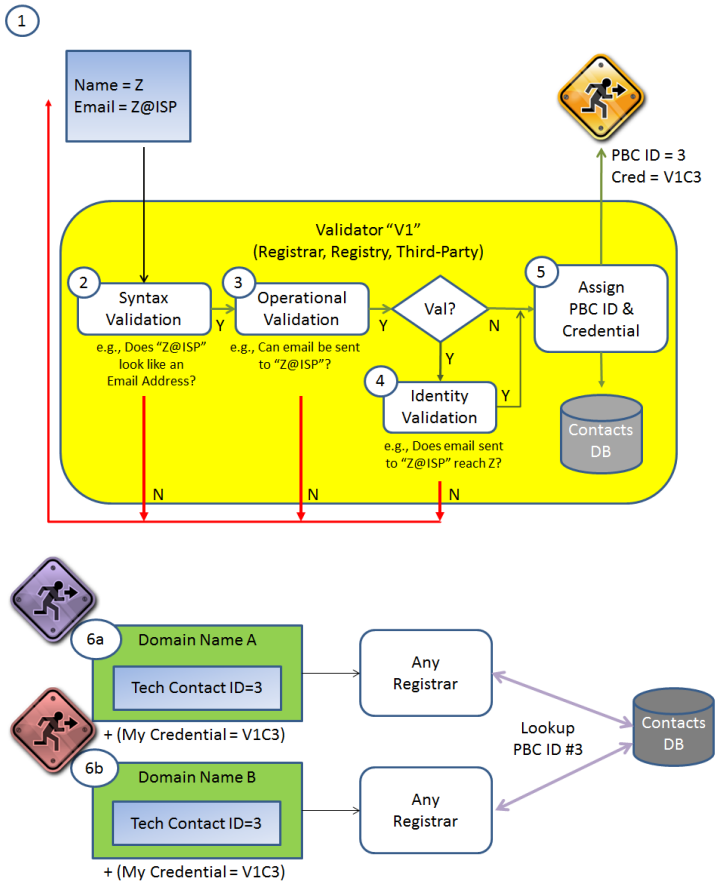
c) **OPTIONAL**: Identity validation may be carried out by the Validators, utilizing entities like post offices, ccTLD managers, telephone companies, tax offices, etc. *Note contacts that have met optional identity validation standards may be designated as such in their status to increase user confidence, which facilitates online commerce. Also note that such value-added services would likely have a cost associated with them that would be borne by the entity requesting this additional level of validation.*

d) After a successful syntactic validation and any required operational validation, an identifier is issued to the block of contact data (Contact) by the Validator, uniquely identifying both the Validator and the Contact to enable subsequent retrieval and update.

e) The Validator stores the contact data in its own database, issues credentials (as applicable, to enable future update to the Contact), and relays the unique identifier to the applicant (from here on known as the Contact Holder).

f) The Contact Holder provides this Contact ID to Registrants, who may then proceed to any Registrar, using this unique identifier, to register domain names using Contact IDs as designated Purpose-Based Contacts (i.e., PBCs). *As defined in Section III, an authorization process must be engaged to ensure the Registrant and designated Contact agree on the purposes that PBC will accept for each domain name.*

g) Validated Contact IDs can be designated as PBCs for a domain name (e.g., Registrant, technical, admin, business, abuse, legal, Privacy/Proxy provider) following the principles for Purpose-Based Contacts as defined in Section III(e).



Note that each Validator maintains its own Contacts database. This data must also be provided to the RDS, but that mechanism depends upon the RDS model as described in Section VII. For example, in the Synchronized model, contact data additions and updates might be pushed via EPP to the RDS. In the Federated model, contact data might be pulled by the RDS in real-time via RDAP.

c. Accuracy, Audit, and Remediation Process

The following processes are recommended to ensure continued accuracy of registration data and remediation of inaccurate registration data:

a) **Self-correction**: Contact Holder uses Validator to correct /update their data using their previously issued credentials. Information automatically flows across to all domains utilizing that particular contact (as designated by the unique Contact ID).

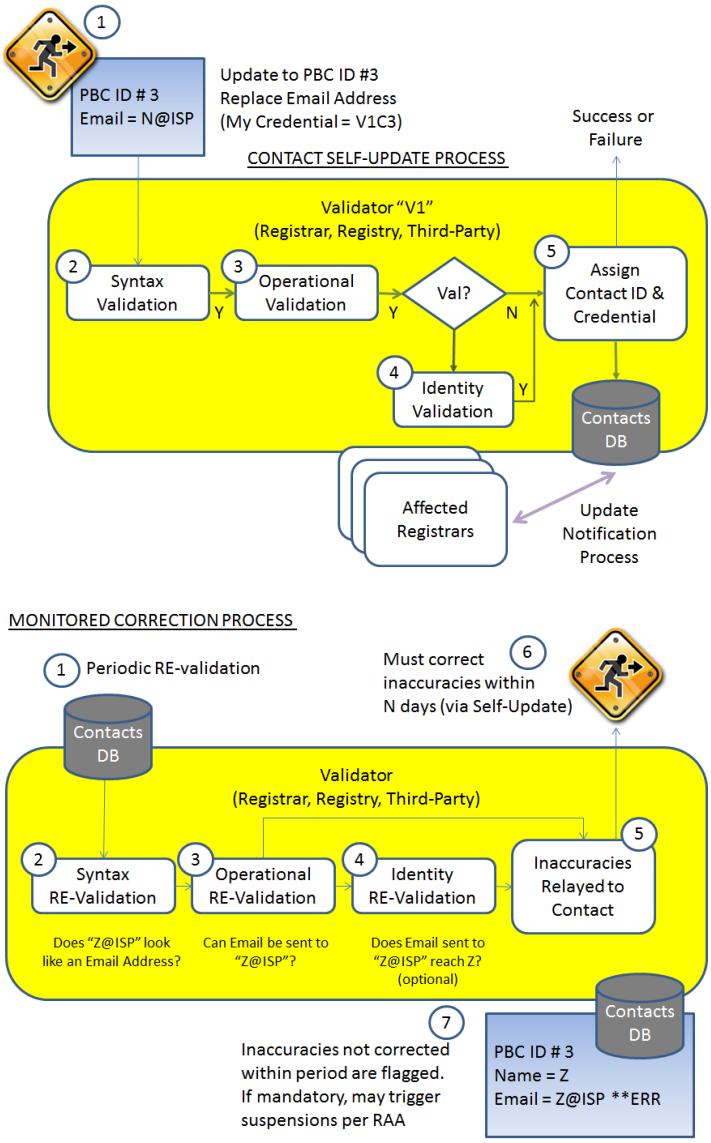
b) **Monitored process**: Validators conduct periodic operational and optional identity validation on contact sets managed via their service. *Note: Such validation procedures should not be overly burdensome, but could be reflected in statuses published for any contact (e.g. Contact is operationally valid as of Jan 1, 2016).*

c) Validators report any inaccurate data detected to the Contact Holder, giving a specific period of time (for example, 14 days) for the Contact Holder to correct the inaccuracy. Registrants, Registries, and Registrars of any affected domains may be notified. The Contact Holder uses their previously chosen Validator to correct the inaccuracy using their previously issued credentials.

d) If the registration data remains inaccurate after the deadline, the data is flagged as inaccurate. If the flagged data is mandatory for any PBC currently referencing this Contact ID, then the associated domains are put into a remediation process that would notify the Registrant of the inaccuracy and allow them to rectify it in the RAA-specified time period. Failure to correct could lead to sanctions for the domain name that may include suspension or deletion as per the applicable RAA.

e) Once the flagged data is replaced with valid data, any sanctions are removed from affected domains.

f) In the case of accuracy reports submitted to ICANN compliance, the Validator will be notified to repeat syntactic and operational validation. If re-validation succeeds, the party submitting the accuracy report may take other actions as appropriate to their situation (e.g., filing a UDRP complaint or submitting a Reveal request). If re-validation fails, the Registrants of all domain names using that inaccurate Contact ID must be notified and follow the normal remediation process outlined above.



d. Operational Framework for Contact IDs

The following framework is recommended to manage Contact IDs and associate them with registration information:

a) Contact IDs must be unique across all Validators to ensure Contact ID portability and provide definitive mappings between domain names and necessary directory information.

b) Contact IDs which identify both the Contact and Validator must be associated with discrete blocks of contact information to enable retrieval and update. Explanation: a Contact ID maps to a set of contact data that is usable for communicating with designated domain name contacts. Information that falls short of this requirement is operationally useless.

c) Contact IDs must be issued by accredited Validators. Any entity may apply to become a Validator, subject to criteria analogous to that now used to accredit Registrars. Accredited Validators may include Registrars, Registries, and third party validation providers. Rationale: a Validator is a necessary function of creating a contact database. The level of validation may vary by contact, but the process needs to be harmonized among Validators to ensure accuracy and accountability to domain Registrants and their designated contacts.

d) To be associated with a domain name, a Registrant or designated PBC must obtain a Contact ID.

e) Contact IDs may be assigned to multiple roles for one or many domains. E.g., a given PBC ID may be used as a Registrant ID for one domain, and a Tech and Abuse Contact for other domains.

f) Contacts may be created and modified at any time, including as part of the domain registration process.

e. Interaction with Validators

The EWG recommends the following principles for Validator interaction with Contact Holders (i.e., parties that successfully create validated, reusable blocks of contact data.)

No.	Principles for Interaction between Contact Holders and Validators
83.	For any given Contact ID, a Contact Holder may choose any Validator[19].
84.	Oversight and accountability policies related to the management of Contact IDs must be developed.
85.	Contact Holders must be able to modify the contact information associated with a Contact ID through the issuing Validator.
86.	Validators must use Contact Holder authentication to deter unauthorized modification of contact information associated with a Contact ID.
87.	Validators may offer multiple levels of Contact Holder authentication, ranging from basic PIN authentication to two-factor authentication. Contact Holders must be able to choose providers based on cost/benefit propositions tied to ease-of-use, security, costs, and other logical business factors.

[19] Per principle #88, Contact IDs identify both the Validator and the Contact Holder. This should be implemented in a way that enables Contact ID portability between Validators.

No.	Principles for Interaction between Contact Holders and Validators
88.	Validators must publish their policies on authentication in a manner that can be utilized globally for reputation management. This will encourage better accuracy and accountability for listed contact information.
89.	Validators must be able to validate contact information submitted in the Contact Holder's native language. This should improve accuracy of native-language data and support scalability of the domain name registration system into a multi-lingual environment. For example, Registrars could work with Validators in various localities to provide expanded validation services to large numbers of Registrants and designated contacts without having to invest in costly tools to validate data in languages unfamiliar to their own staff.

f. Principles for Contact Validation

Contact data can be validated at three different levels: syntactic, operational, and identity, as per SAC 058. The EWG recommends the following validation-level principles.

No.	Principles for Contact Validation
90.	All contact data elements associated with a Contact ID must be validated at a syntactic level. This represents a base-level of validation that must be achievable by any entity in the industry.
91.	All mandatory contact data elements associated with a Contact ID for a particular purpose must be validated operationally[20] before that Contact ID can be included in domain name registration data for that purpose.
92.	A Contact Holder may voluntarily seek optional higher levels of validation (e.g., optional identity validation), bearing associated costs in return for perceived benefits (e.g., greater consumer confidence in domain names registered to identity-validated entities)[21].
93.	Given costs involved with optional identity validation, a low-cost mechanism for economically disadvantaged Contact Holders to receive optional identity

[20] Refer to SAC 058 and *ccTLD WHOIS Data Verification/Validation Survey Results Summary* for possible ways to implement operational validation and existing ccTLD practices.

[21] For example, optional identity validation could be a separately-priced add-on or bundled into domain name registration packages or offered as an incentive to high-volume customers. Refer to *RFI on Contact Data Validation and Verification Systems* for examples of commercial services that perform such validation.

No.	Principles for Contact Validation
	validation is desirable.
94.	In order to preserve associations and allow for a correction process, a Contact ID can have a status of "inaccurate" and remain in the system.
95.	Validation Status of the Contact ID must be tracked and published as appropriate when accessing RDS information, along with the most recent time the validation status was determined.
96.	Third parties may file inaccuracy reports to challenge the Validation Status of a Contact ID as described in Section V(c), triggering a standard remediation process that may result in the Contact ID being flagged as "inaccurate" and in further consequences for domain names using that Contact ID as a PBC.
97.	Active domains cannot have a mandatory contact with an "inaccurate" status without some sort of remediation. The scheme can be determined elsewhere, however.
98.	A minimum level of cross-field validation must be checked for all contact data elements associated with Contact IDs where cross-field validation is applicable (e.g. physical address).
99.	Revalidation of contact data must be carried out on a regular basis by the applicable Validator to ensure data is accurate at the declared level.
100.	If a Contact Holder provides optional data elements, those elements must be at least syntactically validated. Optional data elements would not be validated beyond syntax unless the Contact requests and presumably pays any costs associated with such validation.
101.	The level of validation achieved beyond syntactical validation for data elements that can be operationally- or (optionally) identity-validated must be recorded and maintained by the Validator. For example, elements like email, phone, and address could be operationally-validated, while a name or organization name could not be operationally-validated but could optionally be identity-validated.
102.	In addition, the Validator must determine and publish as an RDS data element the overall validation status achieved by each Contact ID. For example, if ALL mandatory data elements that can be operationally-validated pass those checks, the Contact's overall validation status would be "operationally validated." If ANY mandatory data element that can be operationally-validated fails, the Contact's overall validation status would be down-graded to "syntactically validated." If ALL

No.	Principles for Contact Validation
	mandatory data elements that can be identity-validated pass that optional check, that Contact's overall validation status would be upgraded to "identity validated." To promote accuracy and efficient communication, this overall validation status must be made available to RDS users as one new consolidated data element per Contact.[22]
103.	For any data element that has undergone validation, the timestamp of that validation must also be recorded and maintained by the Validator.
104.	The timestamp of the most recent change to the overall validation status for an entire Contact ID must be also be determined by the Validator and published as a new RDS data element per Contact.

g. Unique Contact Data Capability

In order to combat impersonation, defamation, and abuse, a Contact Holder may designate that their contact data is unique and must not be used by other Contact Holder claimants.

a) Unique data could include many elements of a contact set, particularly email address and phone number. Uniqueness of addresses and names may be difficult to impossible to guarantee.

b) If a Contact Holder requests a uniqueness designation, there must be a mechanism provided for other Validators to compare a requested set of contact data against the Contact Holder's, to ensure that new Contact ID applicants (or existing Contact Holders modifying their information) do not impinge upon uniquely protected data.[23]

c) Any data designated as unique must be identity-validated to prevent impersonation and "denial of service" type attacks (legitimate contact unable to use their true data).

---

[22] The EWG also considered publishing RDS data elements to convey the individual validation status of each individual contact data element (e.g., PBC email address status = operationally-validated, PBC name status = identity-validated). Publishing validation status at this granularity would require significant protocol, data element, and client application/GUI changes and so is not recommended at this time, but may warrant further study.

[23] This uniqueness check can be performed relatively easily in the Synchronized RDS model, but may be more challenging to perform in the Federated RDS model.

h. Summary of Data Quality Key Benefits

Adopting Contact ID Management and Validation systems as an integral part of the next-generation RDS will improve data quality by making it more difficult for Registrants to insert false data into the RDS and reducing the incidence of fraud and identity theft. Specifically, benefits of adopting the EWG's recommended data accuracy and validation principles include the following.

- Increased ability for individuals and organizations to control and maintain their own contact data no matter where it is used in the domain name ecosystem.
- Making it more difficult for miscreants to obtain domain names, as all contacts must be validated to a minimal level upon creation or updates. Validator accreditation requirements should allow for identification and sanctions of rogue or lax Validators that do not meet operational standards. Should miscreants be identified via a single domain registration, other domains held by the same miscreant may be identified and mitigated via common PBCs.
- Creating more consistent data across multiple domain names registered by a given Registrant. While there may be some up-front costs of validation for a given contact, providing a single, portable Contact ID allows for frictionless additional registrations and should greatly reduce future maintenance costs for many Registrants.
- Improved ability to detect invalid contact information over time and apply fixes to the entire set of domains using that contact information. Requirements for periodic validation checks by Validators, or whenever updates are made, should highlight problems with out-of-date contact information and apply all updates to all affected domain name registrations with a single change.
- Cost and efficiency improvements for the entire ecosystem. While introducing new complexities to the overall registration system, contact management can be separated from domain registration management, allowing large-scale updates to be applied to domains while permitting localization of the contact data management.
- Ability for service providers to seamlessly update contact details without having to update individual domain registrations for domains in which they appear as a Purpose-Based Contact. In many providers' situations, this could allow for easy updates to thousands or even millions of domain names.
- Reduce abuse occurring via impersonation in registration data by providing optional identity validation. While optional identity validation will likely incur

costs to a Contact Holder who obtains it, the ability to curtail abuse via impersonation (identity theft) routinely experienced by high profile entities, large service providers, or maliciously-targeted individuals, would be well worth the expense.

- Separation of contact data management and validation from domain name registration/management more closely aligns data subjects with their data, allowing for easier application of relevant data protection law as Validators can be located in jurisdictions local to a Contact Holder, regardless of Registrar or Registry location.
- Validators can provide services in native languages to Contact Holders and Registrants, improving data quality and accuracy, thus reducing costs for validation. This could allow Registrars to offer services in languages they could not easily support or validate on their own, via a distributed set of Validators.

VI. Legal and Contractual Considerations

In its work, the EWG has been guided by some overarching legal principles:

Personal data must be: • processed lawfully, fairly and in a transparent manner in relation to the data subject, • collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes, • adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed, and • accurate and kept up-to-date as required for the specified purposes.
Lawful processing, including transfer and disclosure can be – subject to the relevant jurisdiction – based on: • consent of the data subject, • the necessity for the performance of a contract to which the data subject is party, and • the necessity for compliance with a legal obligation to which the controller is subject.
A right of access to information and a right to rectify inaccuracy for the data subject have to be ensured.

The EWG recommends that these and other related principles normally found in data protection law should be considered when drafting final policies and implementation processes for the RDS. In addition, it is well recognized that, in some jurisdictions, privacy rights extend to legal persons and to entities with respect to free speech and freedom of association. The EWG recognizes both of these separate sets of rights, which are protected separately and differently around the globe.

Given this foundation, the EWG assessed options and then formulated RDS principles for privacy and data protection, and for law enforcement access. Those EWG principles are presented in this section, supported by principles for contractual compliance, accountability, and audit.

a. Data Protection Principles

Today, practices that purport to address applicable national law on privacy and consumer protection are uneven. Some laws require that when data is exported outside the jurisdiction of the individual or of the data processor governed by that law, similar or equivalent data protections be applied. The European data protection directive of 1995 does not allow for data transfer outside that jurisdiction unless local law was evaluated as "adequate." Many other jurisdictions outside the EU have looked for strong contractual provisions, but in any case most laws demand that those who are holding personal data not transfer or disclose it to others without consent unless protection is guaranteed. Liability can accrue at this transfer point. At the moment, ICANN has addressed this by permitting a waiver in the RAA contract to Registrars who demonstrate they are subject to data protection law which would prohibit data escrow. This is not the only provision in the ICANN ecosystem which represents a risk to those seeking to adhere to data protection law, so it has been suggested that the status quo needs to be carefully examined. Given the focus the EWG has taken on accountability in its work, the requirement to be accountable for data protection has been examined.

At the moment, requirements that the entity receiving personal data must guarantee protection that is adequate and consistent with the protections provided to the data subject "at home" would have to be fulfilled on a **case-by-case** basis, depending on whether the entity receiving data is in a jurisdiction that provides legislated data protection or similar adequate protection. This means that either the adequacy is ensured by the law applicable to the entity that receives the data or other guarantees are put into place allowing for the data transfer to be legal under the law applicable to the data subject.

Data Protection Mechanisms

Given the current situation, four incremental options for protecting personal data throughout the RDS ecosystem were examined:

(0) do nothing;

(1) introduce mechanisms to facilitate routine legally compliant data collection and transfer;

(2) introduce mechanisms that seek to harmonize privacy and data protection throughout the ICANN ecosystem, to provide a basic "floor" of data protection that establishes accepted best practices of privacy policy; and

(3) submit that policy as a set of "binding corporate rules."

Note: Throughout this section, the "RDS ecosystem" refers to all actors enumerated in Section VIII(c) Contractual Relationships and Compliance, and Section VIII(d) Accountability and Audit. This includes ICANN (a U.S. non-profit corporation), all gTLD Registries and Registrars (each of which operate as independent corporations based in many countries), and all new accredited entities proposed by the EWG in this document: the RDS Provider, Validators, Secure Protected Credential Approvers, RDS User Accreditors, ICANN Compliance, and any other entity involved in handling personal data.

Option (0): "Do nothing"

Doing nothing would result in very high complexity because of the continuing risk of non-compliance with data protection law and the necessity of examining each registration to determine applicable law. It would create costly overhead for some operators, notably Registries. For Registrars it could impose the high cost of monitoring the adequacy of protection required by Registrants and Registries. It would add the potential of legal uncertainty for all parties, including ICANN and other stakeholders in the Domain Name System. The increase in the number of gTLDs and the variety of Registry locations creates new challenges regarding applicable law and jurisdiction for ICANN's contractual regimes as they pertain to Registrant privacy and consumer protection. Clutter, uncertainty, and uneven practices would require more effort from ICANN to ensure contractual compliance and reduce potential risk. These challenges exist independently from the question of an RDS. With the introduction of 1000+ gTLDs, the issue becomes more acute. Most importantly, protection of the data subject cannot be consistently guaranteed. A framework for harmonization which reduces risk, minimizes burden, and decreases complexity is in the interest of every stakeholder.

Option (1): Introduce mechanisms to facilitate routine legally compliant data collection and transfer

The second option considered is the introduction of a system which would assess the relevant privacy and data protection law and present the legislation in a list so that stakeholders could apply it, and individuals could be aware of where their data was and which law applied. This list could be applied automatically by the RDS through a "rules engine" as defined in the next section. If an individual lived in a country that had data protection law, and that law applies outside the country to personal data transferred from the individual to another party (in this case the Registrar) that law might apply. If the Registrar was located in a country whose data protection laws applied to all

individuals (i.e., not just its own citizens) then that law would certainly apply. The data in question or in scope for our purposes is only that which is collected in the RDS[24]. Coding the data about the jurisdictions which apply in the ecosystem would make life simpler for the stakeholders involved, would assure data protection rights (if applicable) for the Registrant, and would reduce risk of non-compliance. However, in jurisdictions without data protection law that applies to the domain name registration business, Registries, or ICANN and its compliance mechanisms, this scenario provides little protection to the individual Registrant. This could result in a multi-tiered system of privacy rights, with some individual Registrants having none and others having full human rights and a cause of action with judicial oversight.

Option (2): Introduce mechanisms which would seek to harmonize data protection throughout the RDS ecosystem to provide a basic "floor" of data protection that looks after accepted best practices of privacy policy.

Contractual clauses could be crafted to rectify any gaps in privacy protection (further discussed under implementation), and these clauses could be based on a commonly accepted suite of privacy protections, which would form the basis of an ICANN privacy policy. This policy could be concise, listing the relevant clauses in an appendix. This could allow for the unfettered transfer of data between RDS ecosystem actors by providing a level of data protection that is high enough to prevent objections for reasons of personal privacy, data protection, and consumer rights.

Mechanisms to facilitate legally compliant data collection and transfer throughout this RDS ecosystem could take different forms, but they would all be based on a consistent data protection policy applicable to the RDS. ICANN would enforce this policy with all stakeholders through contractual provisions, as it does most other policies.

Option (3): Building on (2) above, the policy developed could be submitted as a set of "binding corporate rules," as recognized by APEC and by the EU in privacy/data protection law.

This option would simplify data transfers among the 28 member countries in the European Union, as it provides a determination of adequate data protection for the EU states' purposes, removing the ad hoc nature of data protection decisions dictated by data flows throughout the RDS ecosystem. While this option might be more time-

[24] This would not necessarily make life less complicated for the Registrar, who controls a lot more sensitive data, such as banking data, credit card information, customer care records, etc., that are not transferred to the RDS, although a "rules engine" would certainly be useful in some situations, given the complexity of the coming gTLD system.

consuming, it could reduce the risk of non-compliance and ensure better protection. It would also provide independent oversight of the privacy policy.

No.	Summary of Data Protection Mechanisms Considered
(0)	Do nothing.
(1)	A minimum solution would a) identify transfers for which adequate privacy protection is ensured by law and publish the respective list; and b) introduce common rules in the contract for those RDS ecosystem actors whose transfers would not be protected by sufficient legal adequacy, giving the compliance function a single and simple platform for maintenance.
(2)	A basic ICANN privacy policy for the RDS could be drafted, based on standard best practices for privacy protection, and standard contractual clauses could be developed which give effect to this policy throughout the RDS ecosystem. Standard clauses could be included in all contracts between ICANN and all RDS ecosystem actors engaged in data transfers, ensuring a sufficiently high level of data protection to permit unfettered transfer within this ecosystem.
(3)	Taking ICANN as a multinational not-for-profit corporation, the entire RDS ecosystem under its control could be subject to the instrument of Binding Corporate Rules (BCRs), which have proven effective in allowing worldwide transfers of data within an organization. In this case, the ecosystem becomes the subject for compliance. ICANN might be seen as acting as "Data Controller," to use the APEC and EU terminology, by setting the policy and the contractual requirements.

Assessment:

Option (0) Do nothing. Given the growing global complexity of the system, and the focus on increased accuracy and accountability, this was considered unacceptable.

Option (1) Mechanisms to facilitate routine legally compliant data collection and transfer. This option would be more complex and more dynamic as laws change in different jurisdictions, and would have to consider a complex data flow within the ecosystem. As discussed previously, an individual Registrant may have a Registrar in a different jurisdiction, use a Validator in a third jurisdiction, maintain data in a Registry in a fourth jurisdiction, and rely on an RDS Provider in a fifth jurisdiction.

Option (2) Standard Contractual Clauses which would seek to harmonize data protection throughout the RDS ecosystem. This choice could require compliance with applicable law for the stated stakeholders, notably Registrants, Registrars, Registries, and ICANN. This could also include the new RDS ecosystem actors recommended in this report: Validators, the RDS Provider, RDS User Accreditors, etc.

In addition to mandating compliance with local data protection laws, this option, in enumerating common elements sourced from APEC and EU data protection law, would do much to ensure compliance. Clauses could specify consent conditions, access rights, retention policies, and other elements by (for example) incorporating EU requirements on legal data processing and appropriate elements addressed by binding corporate rules. Such standard contract clauses would not necessarily require authorization/monitoring by data protection authorities, except in jurisdictions where such authorizations are mandatory.

Option (3) (BCRs for the RDS ecosystem) In addition to mandating compliance with local data protection laws, this option could enumerate common elements sourced from APEC and EU data protection law. As in option (2), clauses could specify consent conditions, access rights, retention policies, and other elements by (for example) incorporating EU requirements on legal data processing and appropriate elements addressed by binding corporate rules. Such standard contract clauses would not necessarily require authorization/monitoring by data protection authorities, except in jurisdictions where such authorizations are mandatory. However, the BCRs would have to be adapted to the specifications of the RDS ecosystem. BCRs are arguably more applicable to corporate entities with a traditional control structure than they are to a loosely-connected ecosystem such as is operated by ICANN, but it is certainly the case that multinational corporations enforce their binding privacy rules through exactly the same kinds of contracts that ICANN uses to accredit and control its stakeholders.

In conclusion, "doing nothing" is not a real option, particularly if the EWG's recommendations for improving accuracy and accountability are accepted. Option (1) would be quite legally complex and does not provide equal rights to all Registrants, while Option (3) raises concerns about applicability within the RDS ecosystem (i.e., are binding corporate rules feasible, would they be accepted, and what would the implications for ICANN be in terms of liability?).

Therefore, the EWG recommends Option (2) – develop a policy using standard contractual clauses that are harmonized with data protection laws to implement the requirements of the policy, and ensure through various audit mechanisms that these

privacy protections are enforced through contracts between all RDS ecosystem actors involved in handling personal information.

Implementation of Data Protection Mechanisms

For all of the above scenarios, the question of RDS implementation is relevant – specifically with regard to the localization of the RDS Provider.

If the RDS is going to hold personal data, it would be convenient if that data were located in a jurisdiction that provided enforceable data protection rights, to avoid questions related to the legality of data transfers and liability for data breach. This issue is clear if the RDS holds data that is resident and co-located with the data processor. A similar framework for consideration should apply, even if the data is not resident but brought there for processing (e.g., validation) and dispatched elsewhere afterwards. Three data protection implementation options were considered by the EWG:

No.	Summary of Data Protection Implementations Considered
(0)	"Do nothing" applies if the level of legal data protection applicable to the localization of the RDS is not taken into account when making the geographic choice. Doing so might result in RDS localization in a jurisdiction with a low level of data protection.
(1)	The RDS could provide for a legal compartmentalization. Specifically, data elements could be tagged according to the applicable law for the data subject (i.e., the Registrant) and treated accordingly. To achieve this legal compartmentalization, the RDS could implement a “rules engine” that would apply the applicable data protection laws to each specific transfer. More specifically, “rules engine” refers to a feature that could be implemented within the RDS to manage (a) the storage, collection and processing of domain name information based on Registrant, Contact, Registrar, Registry, and RDS jurisdictions (represented by the following data elements: Registrant and Contact Country Code, Registrar and Registry Jurisdictions), and (b) data protection laws of the applicable jurisdictions, in accordance with ICANN's future defined policy for the RDS. This is inherently complex, as described above, and difficult to enforce if the RDS were in a jurisdiction without data protection law that provides access to a court.

No.	Summary of Data Protection Implementations Considered
(2)	The localization of the RDS is selected according to the criterion of the easiest and least complicated transfer of data. Doing so would imply selecting location(s) for RDS data storage where the applicable national data protection law provides for a high level of protection.

Assessment:

Option (0) "Do nothing" maintains the status quo and increases the complexity of many data transfers by:

- Reinstating a process that makes it difficult, and in practice almost impossible, to respect legal frameworks;
- Inflicts administrative and legal burdens on Registrars as well as other players in the ecosystem, including ICANN Compliance; and
- Is far from transparent regarding local data protection law and privacy compliance and is not scalable.

Option (1) Legal compartmentalization via a "rules engine" is innovative, but its feasibility would have to be tested technically. Legally, there are a number of open questions, especially regarding the definition, legal acceptance, and implementation of such a system.

Option (2) Data localization in selected jurisidiction(s) could be an elegant and simple solution to afford a very high level of protection for all movement of data. However, this option does not by itself enable application of every subject's local data protection laws.

As option (0) is not feasible, and options (1) and (2) are not mutually exclusive*, the EWG recommends that both options (1) and (2) should be considered at the moment as a means of implementing the high level of data protection to be ensured through policy and standard contractual clauses.*

After considering all of these options surrounding data protection policies, mechanisms, and implementation, the EWG agreed upon the following principles:

No.	Data Protection Principles
105.	Mechanisms must be adopted to facilitate routine legally compliant data collection and transfer between actors within the RDS ecosystem.
106.	Standard contract clauses that are harmonized with privacy and data protection

No.	Data Protection Principles
	laws should be codified in a policy and enforced through contracts between all RDS ecosystem actors involved in handling personal information.
107.	An information system to apply data protection laws (i.e., a "rules engine") and localization of RDS data storage must be considered as two means of implementing the high level of data protection required. This must be ensured through standard contractual clauses, which flow from a logical privacy policy for the RDS ecosystem.

b. Principles for Data Access by Law Enforcement

Unlike in the case of data protection, the legal protection of the data subject in cases of access by law enforcement cannot be "exported." For access by law enforcement, three options are considered.

No.	Summary of Law Enforcement Access Options Considered
(0)	"Doing nothing." Access by law enforcement would follow the existing rules insofar as national law enforcement would have access to RDS data stored in each data repository at the respective national level. At the centralized RDS portal, access would be granted following the national law of the RDS portal's host country.
(1)	At the central RDS portal level, where data are not publicly available and where no specific legal procedures are required from law enforcement under applicable national law, access conditions could be specified for the RDS system and implemented in one of two ways: a) Europol and Interpol could enter into a contractual agreement with the RDS to implement and execute such a system, serving as an active real-time intermediary for all law enforcement access and being accountable for appropriate data protection and use. b) Europol and Interpol could enter into a contractual agreement with the RDS to serve as User Accreditors for the law enforcement community, vetting applicants to issue RDS credentials which are then used by individual agencies to access gated RDS data and be accountable for appropriate data protection and use.

No.	Summary of Law Enforcement Access Options Considered
(2)	Additionally, at the central level, mechanisms could be established that would allow central RDS portal access by law enforcement, even where specific requirements exist in traditional bilateral relations that would be handled by mutual legal assistance treaties (MLATs). A compartmentalization of the data with respect to the applicable law could support the establishment of such a mechanism.

Assessment:

Option (0) ("do nothing") clearly does not provide added access value for law enforcement.

Option (2) (MLATs at the RDS user access portal level) It is not expected that any of the recommended gated data elements made accessible through the RDS would require additional judicial authorisation for law enforcement access. Therefore, option (2) does not need to be considered further.

Option (1) (the accredited RDS user access portal approach) facilitates access by law enforcement. Although both Variants (1a) and (1b) would build upon existing structures, variant (1a) (accredited access with compartmentalization via real-time intermediary) would also build upon existing mechanisms of law enforcement cooperation and avoid creating of an added layer of complexity. However, the ability to detect and remediate potential individual abuses would still have to be ensured.

Variant (1a) s further explored in Section IV(c), RDS User Accreditation, Scenario #3, which details how potential Accreditors such as Interpol might proxy authorized law enforcement access requests to the RDS while still deterring potential abuses. Refer to RDS User Accreditation Principles for related recommendations.

In addition, for option (1), it has to be ensured that the legal framework for national law enforcement in jurisdiction(s) where RDS data is stored does not override the framework established for the RDS. The geography of RDS localisation is therefore critically important.

No.	Law Enforcement Access Principles
108.	The RDS must store data in jurisdiction(s) where law enforcement is globally trusted, regardless of implementation model.

c. Compliance and Contractual Relationship Principles

The EWG recommends the following set of principles around contractual relationships among parties within the RDS ecosystem:

No.	Contractual Relationship Principles
109.	A third party provider that is a non-governmental organization with global scope should operate the RDS.
110.	ICANN must enter into appropriate contracts with the third party provider of the RDS to enable availability, auditing and compliance.
111.	ICANN must enter into appropriate contracts with Validators, Privacy/Proxy Service Providers, Secured Credential Approvers, and others that may interact with the RDS (see Section III(c) Principle #1).
112.	ICANN must amend existing agreements (RAA, Registry Agreements) to accommodate the RDS and eliminate legacy requirements.
113.	The RDS must apply to all gTLD Registries, whether existing, or new. No grandfathering or special exemptions should be allowed.

d. Accountability and Audit Principles

The EWG recommends that RDS ecosystem actors be held accountable for actions taken with registration information, as follows:

No.	Accountability and Audit Principles
114.	All entities within the RDS ecosystem must be held accountable for one or more of the requirements set forth in Table 6: a) provide accurate and reliable registration information b) use the information only for the designated purpose c) secure the information collected, stored, or forwarded d) validate or authenticate the information when collected e) update previously provided information in a timely manner f) enforce RDS privacy policies and Terms of Use (ToU) g) detect abuse of registration information h) address and track complaints i) comply with established ToU and ToS policies j) establish mechanisms to deter third party data harvesting and bulk fraudulent account creation k) establish an on-going auditing and remediation process

No.	Accountability and Audit Principles
	The following stakeholders[25] have accountability roles in the RDS ecosystem: a) RDS Users Seeking Data (USDs) - enumerated in Section III b) Registrants c) Registrars[26] d) Registries[27] e) Registration Directory Service Provider f) ICANN g) Privacy or Proxy Service Providers h) Secure Protected Credential Approver i) Validators j) RDS User Accreditors k) Purpose-Based Contacts l) Escrow Providers
115.	The RDS must establish procedures for handling complaints about unavailability of data, improper use of data, unauthorized access to data, privacy policy breaches, and inaccurate data entry; for example: Abuse Contact data elements, and a portal to capture complaints from USDs and Registrants.
116.	The RDS must establish escalated remedies for inaccurate data; for example: Email Warning, user/browser-visible Flag on Records, ICANN Compliance action, and other new incentives to encourage accuracy. (See Section V Improving Data Quality for accuracy requirements.)
117.	The RDS must establish escalated remedies for unauthorized access to data; for example: Email Warning, Rate Limiting, Temporary Blocking, Accreditation Suspension, Termination, and other deterrents. (See Section IV Improving Accountability for gated access requirements.)
118.	The RDS must establish escalated remedies for improper use of data; for example: Email Warning, Rate Limiting, Temporary Blocking, Accreditation Suspension, Termination, and other disincentives. (See Section III Users and Purposes for permissible purposes.)
119.	The RDS must establish audit mechanisms in order to detect abuse of RDS

[25] These roles and responsibilities extend to stakeholder agents, and assigns (e.g., Resellers)

[26] As defined by http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.htm

[27] As defined by http://newgtlds.icann.org/en/applicants/agb/agreement-approved-09jan14-en.pdf

No.	Accountability and Audit Principles
	Access Credentials and ToU violations; for example: mechanisms to detect unusual behaviour patterns. (See Section IV Improving Accountability for RDS User Accreditation requirements.)
120.	The RDS must establish audit mechanisms in order to detect abuse of registration data for uses other than stated purposes; for example: mechanisms to detect unusual behaviour patterns. (See Section III Users and Purposes.)
121.	The RDS must establish audit mechanisms in order to detect abuse by Validators; for example: training of Validators, periodic random sampling of data to be checked to ensure proper validation. (See Section V Improving Data Quality)
122.	The RDS must establish audit mechanisms in order to detect abuse by RDS User Accreditors; for example: establish mechanisms to detect unusual behaviour patterns. (See Section IV Improving Accountability for definition of abuses.)
123.	The RDS must establish audit mechanisms in order to detect abuse by Privacy/Proxy Providers and Secure Credential Approvers; for example: establish mechanisms to detect unusual behaviour patterns. (See Section VI Improving Registrant Privacy for definition of abuses).
124.	RDS USDs must agree to the auditing of data access, use and provision of accurate identity and purpose information in Terms of Use (ToU).
125.	The RDS must establish a process for remediation, suspension or termination of Validators if data is not properly validated, stored and secured. (See Section V Improving Data Quality for VR requirements.)
126.	The RDS must establish a process for remediation, suspension or termination of Secure Credential Approvers if vetting is not proper or adequate. (See Section VII Improving Registrant Privacy for requirements.)
127.	The RDS must establish a process for remediation, suspension or termination of RDS User Accreditors if USDs are not properly accredited, stored and secured. (See Section IV Improving Accountability for RDS User Accreditor requirements.)

No.	Accountability and Audit Principles
128.	ICANN must establish ToS policies for ensuring the Registries, Registrars, and Validators provide accurate, updated and timely data to the RDS. (See Section VI Legal and Contractual Considerations for RDS and Registry requirements, to be reflected in the RIA and RAA.)
129.	The RDS must establish an audit process for Registries, Registrars, and Validators and a process for reporting to ICANN if the Registry/Registrar/Validator is not providing accurate, updated and timely data. (See Section VI Legal and Contractual Considerations for RDS and Registry requirements, to be reflected in the RIA and RAA.)
130.	The RDS must establish audit mechanisms to ensure the ongoing quality and integrity of the data collected by the RDS and stored with the Escrow Provider. (See Section VIII Data Storage Escrow and Logging)
131.	ICANN must establish audit mechanisms in order to detect breaches of any ToCs by the RDS Provider. For example: allows unauthorized use of data, does not respond to complaints concerning abuse of data, abuse of credentials or abuse of validation. (See Section VI Legal and Contractual Considerations)
132.	ICANN must establish a process for remediation, suspension or termination of the RDS Provider if not fulfilling contractual responsibilities. For example: availability, reliability, privacy, access rights, and performance requirements. (See Section VI Legal and Contractual Considerations)
133.	ICANN must define and benchmark annual improvements made towards achieving the major goals of the RDS: (I) improved data quality, (ii) improved accountability, (iii) improved privacy. The RDS must demonstrate sustained progress in all three areas at similar rates, with a process to identify and remediate unforeseen problems that cause any area to improve more slowly than the others.

The following table summarizes RDS ecosystem entities and the types of accountability and audit requirements that should be applied to them, expanding upon Principle #114.

Applicable Requirements	RDS User Seeking Data	Registrant	Registrar	Registry	RDS Provider	ICANN	Privacy Proxy Provider	Secure Cred Approver	Validator	RDS User Accreditor	Purpose-Based Contact	Escrow Provider
Provide accurate/reliable data		✔	✔	✔	✔		✔	✔	✔		✔	✔
Use for designated purpose	✔		✔	✔	✔	✔	✔	✔	✔			✔
Secure information			✔	✔	✔	✔	✔	✔	✔			✔
Validate/Authenticate					✔				✔	✔		
Timely updates		✔	✔	✔			✔	✔	✔		✔	
Enforce privacy policies			✔	✔	✔	✔	✔	✔	✔			✔
Detect abuse					✔	✔				✔		
Complaint process			✔	✔	✔	✔	✔	✔	✔	✔		
Deter third party harvesting				✔	✔				✔			
Audit and remediation					✔	✔				✔		

Table 6: Compliance Requirements on RDS Ecosystem Entities

VII. Improving Registrant Privacy

Central to the remit of the EWG is the question of how to design a system that increases the accuracy of the data collected, while also offering protections for Registrants seeking to guard and maintain their privacy. The EWG recognizes that personal information is protected by data protection law, and that even where there is no law, there are legitimate reasons for individuals to seek heightened protections of their personal information. In addition, some businesses and organizations may seek protection of their information for legitimate purposes, such as when they are preparing to launch a new product line, or in the case of small businesses, where contact information discloses personal data.

Accordingly, the EWG recommends the following basic principles:

No.	Privacy Principles
134.	In addition to the privacy afforded by compliance with data protection laws, the RDS ecosystem must accommodate needs for privacy by including: • An accredited Privacy/Proxy Service for general personal data protection and adherence to local privacy law; and • An accredited Secure Protected Credentials Service for persons at risk, and in instances where free-speech rights may be denied or speakers persecuted.
135.	There must be accreditation for Privacy/Proxy service providers and rules regarding the provision and use of accredited Privacy/Proxy services.
136.	Outside of domain names registered via accredited Privacy/Proxy services, all Registrants must assume responsibility for the domain names they register.
137.	ICANN must investigate the development of a single, harmonized privacy policy which governs RDS activities in a comprehensive manner, as discussed below.

In addition to data protection laws, other national privacy laws and constitutions protect the rights of hundreds of millions of Internet users to speak online and express their views without their opinions being easily and immediately traced to their names and addresses. These privacy laws include the UN Declaration of Human Rights (Article 19)[28] which protects the rights of freedom of expression and free speech, and preserves the

ability and even the obligation of groups, organizations, individuals, and companies (such as media and journalism companies) to review, criticize, and critique the practices of leadership, exercise of leadership and running of a country, culture or society.

Privacy laws that protect free speech and freedom of expression often recognize the need to exercise these rights under rules that dissociate the names and addresses of the organizations and groups from the speech they are issuing and that may be critical of a government, society, community or neighborhood. They may encourage the marketplace of ideas, and place the needs of open societies to communicate above the authority to persecute speakers or the possibility of pre-judging a message simply because someone does not like its proponent.

Privacy laws and constitutional rights may also protect freedom of association, religion, ethnicity, morality and community. Collectively, they may bar the need of individuals or organizations to declare their names or even addresses in the exercise of unpopular or minority views – so that they may not be immediately tracked down and disparaged, or worse. In this decade of grass-roots political unrest and antagonism to any opposing view, privacy laws protect minority voices and preserve the ability of online speakers to powerfully urge change and reform.

Throughout this report, it is recognized that when we speak of privacy and protection of personal information, we mean to recognize both these separate sets of rights, which are often protected through different legislation, and are done so differently around the globe.

a. Accredited Privacy and Proxy Service Principles

Currently, there are services offered to obscure the identity and/or address of entities using domain names. These developed because of the open nature of WHOIS. While there are many variants, the 2013 Registrar Accreditation Agreement defines two such services:

- A "Privacy Service" is a service by which a Registered Name is registered to its beneficial user as the Registered Name Holder, but for which alternative, reliable contact information is provided by the P/P Provider for display of the Registered Name Holder's contact information in the Registration Data Service (WHOIS) or equivalent services.
- A "Proxy Service" is a service through which a Registered Name Holder licenses use of a Registered Name to the P/P Customer in order to provide the P/P Customer use of the domain name, and the Registered Name Holder's contact information is displayed in the

> Registration Data Service (WHOIS) or equivalent services rather than the P/P Customer's contact information.

In these definitions, "P/P Provider" or "Service Provider" is the provider of Privacy/Proxy Services, including a Registrar and its Affiliates, as applicable. "P/P Customer" means, (regardless of the terminology the P/P Provider uses), the licensee, customer, beneficial user, beneficiary, or other recipient of Privacy Services and Proxy Services.

Today's privacy or proxy services are not standardized; providers have no contractual relationship with ICANN, although the 2013 RAA introduces the concept of accreditation by ICANN and a baseline of obligations, as reflected in an Interim Specification. However, some providers are also Registrars. All Registrars are subject to the RAA, which states the following about proxy-registered domain names:[29]

> 3.7.7.3 Any Registered Name Holder that intends to license use of a domain name to a third party is nonetheless the Registered Name Holder of record and is responsible for providing its own full contact information and for providing and updating accurate technical and administrative contact information adequate to facilitate timely resolution of *any problems that arise*[30] in connection with the Registered Name. A Registered Name Holder licensing use of a Registered Name according to this provision shall accept liability for harm caused by wrongful use of the Registered Name, unless it discloses the current contact information provided by the licensee and the identity of the licensee within seven (7) days to a party providing the Registered Name Holder reasonable evidence of actionable harm.

WHOIS for a domain registered today by a proxy service may look something like this:

```
Domain Name: EXAMPLE-DOMAIN.COM
    Created on: 31-Oct-11
    Expires on: 31-Oct-13
    Last Updated on: 19-Sep-12

 Registrant:
 Domains By Proxy, LLC                        ← Registrant Name = Proxy
 DomainsByProxy.com                           ← Registrant Org = Proxy
 14747 N Northsight Blvd Suite 111, PMB 309   ← Registrant Address = Proxy's
 Scottsdale, Arizona 85260
 United States

 Admin Contact: [same for Tech Contact]
    Private, Registration
```

[29] The new 2013 RAA was approved by the ICANN Board on 27 June 2013; Section 3.7.7.3 (quoted here) is largely unchanged from the 2009 RAA, except for the addition of the 7 day time period.

[30] Note: The EWG suggests that ICANN consider whether "any problem" might be overly broad.

```
example-domain.com @domainsbyproxy.com          ← Email = domain@proxy
Domains By Proxy, LLC                           ← Name = Proxy
DomainsByProxy.com                              ← Org = Proxy
14747 N Northsight Blvd Suite 111, PMB 309      ← Address = Proxy's
Scottsdale, Arizona 85260
United States
(480) 624-2599      Fax -- (480) 624-2598       ← Tel/Fax = Proxy's
```

WHOIS for a domain registered today using what is currently called a privacy service looks similar, except that the Registrant Name (and often Admin/Tech Contact Names) directly identify the privacy service customer, not the proxy service provider.

There are no standard processes employed by all of today's privacy and proxy service providers. However, there are several common needs, often supported to some degree:

- Relaying communication to today's privacy or proxy service customer – often done by auto-forwarding email sent to the admin/tech contact's email address. Relay is provided by many but not all providers.
- Revealing the identity of the licensee and direct contact detail for a proxy customer in response to a complaint about the domain name. Processes, documentation, responsiveness, and actions taken vary and often depend on established relationships between requestors and providers.
- Unmasking the identity of the licensee, making the name and contact details of the proxy service customer publicly available in the WHOIS.
- When requestors can't contact a proxy service customer or get a resolution from the proxy service provider, they often turn to the Registrar (which may or may not be affiliated with the proxy service provider).

Shortcomings in today's privacy and proxy services are well documented.[31] To address both domain name Registrant and stakeholder needs for more uniform and reliable Privacy and Proxy Services which enable greater accountability, the EWG recommends the following principles:

[31] See **Annex B** for studies and reports that document deficiencies with WHOIS as well as Privacy/Proxy services.

No.	Accredited Privacy/Proxy Services Principles
	General
138.	ICANN must accredit Privacy and Proxy service Providers[32].
139.	At minimum, the accreditation program must continue the Privacy/Proxy commitments under the 2013 RAA Specification.
	Principles for Accredited Privacy Services
140.	Entities and natural persons may register domain names using accredited Privacy services that do not disclose the Registrant's contact details except in defined circumstances (e.g., terms of service violation, subpoena).
141.	ICANN must require specific terms to be included in the terms of service. The terms of service must include requiring the service provider to endeavor to provide notice in cases of expedited take-downs.
142.	Accredited Privacy services must provide the Registrar (using a PBC created through a Validator) with accurate and reliable contact details for all mandatory Purpose-Based Contacts, in order to reach the Privacy service provider and entities authorized to resolve technical, administrative, and other issues on behalf of the Registrant.
143.	Accredited Privacy services must be obligated to relay emails received by the Registrant's forwarding email address to the Registrant.
	Principles for Accredited Proxy Services
144.	Entities and natural persons may register domain names using accredited proxy services that register domain names on behalf of the Proxy service customer.
145.	Accredited Proxy service providers must provide the Registrar (using a PBC created through a Validator) with their own Registrant name and contact details, including a unique forwarding email address to contact the entity authorized to register the domain name on behalf of the Proxy service customer.
146.	As the registered name holder, accredited proxy service providers must assume all the usual Registrant responsibilities for that domain name, including provision of accurate and reliable mandatory Purpose-Based Contacts and other registration data.

[32] The GNSO has formed a working group to develop policies for Privacy/Proxy Service Accreditation. The EWG recommends that the RDS reuse any foundation established by the PPSAI WG, modified as needed to reflect RDS access methods and data elements – most notably, P/P published Purpose-Based Contacts.

No.	Accredited Privacy/Proxy Services Principles
147.	Accredited Proxy services must provide the Registrar (using a PBC created through a Validator) with accurate and reliable contact details for all mandatory Purpose-Based Contacts, in order to reach the Proxy service provider and entities authorized to resolve technical, administrative, and other issues on behalf of the Proxy service customer.
148.	Accredited Proxy services must be obligated to relay emails received by the Registrant's forwarding email address as further described in Annex H.
149.	Accredited Proxy services must be obligated to respond to reveal requests in a timely manner as outlined in the escalation procedures described in Annex H.

b. Secure Protected Credential Principles

It has been recognized that some individuals and groups who wish to maintain their anonymity on the Internet, or at least avoid their address and personal information becoming available to those who could be a threat to them, have a legitimate need for heightened privacy protection. These parties may exercise their rights under privacy law where it exists or use proxy registration services. But unfortunately these mechanisms may not be secure enough for those who are genuinely under threat. If the Registrant's details are not available on the Internet, the pursuers of these individuals or groups will target the Validators, the Registrars, or the Registries with their requests for information, often using social engineering techniques that these parties are ill-equipped to detect.

The goal of offering secure protected credentials is to provide safe anonymous registration for individuals or groups under threat. This may include those who wish to exercise free speech (which is widely regarded as protected), or speakers whose identification could cause a threat to their lives or those of their families.

Here are five different examples:

1. Religious minorities

In many jurisdictions there are religious minorities who are under threat from groups in the larger population or from elements in their own faith. They may wish to have a website to provide information to their members, yet maintain secrecy as to where and how they operate. For example, a synagogue in Rome does not disclose its address because of frequent bomb threats, yet publishes service times for members who know its location.

2. Domestic abuse

Many jurisdictions provide some form of identity change for persons who have suffered domestic abuse or who flee their aggressors. This also applies to those who flee certain religious communities and cults and to those under witness protection programs. Shelters for women who suffer domestic abuse may need to advertise their services on the Internet and secure contact points and directions for genuine victims to reach the facility, etc. Individuals and families that have changed identities may have legitimate desires to set up websites without ever disclosing their true address and identity. It should be noted that there are many individuals working for governments who operate under changed identity for various reasons, usually related to national security and law enforcement, and these individuals also need enhanced protection both in the field and in their private lives.

3. Political Speech

In several countries around the globe, an opposition party or unsuccessful candidates may flee after an election. They may also wish to run a website where they can provide details on events in their home country or the persecution to which they are subjected. The government in power may pursue the website, alleging treason or other crimes, after documentation of its abuses appear on the website. These are delicate situations, as free speech rights vary hugely from state to state and rarely stand up against allegations of treason. The right to register a domain is all that ICANN and its accredited Registrars need to be concerned about.

4. Ethnic or other social groups

Ethnic groups often suffer harassment and discrimination and may wish to run websites where they provide vital information for their members. For instance, they may wish to run a website where members can post incidents of harassment without fear of identification and reprisal. Other groups, such as gay, lesbian, or transgendered, may wish to run a very ordinary informational website for their community, yet fear the identification of members because of restrictive laws in their country or reprisals from vigilantes or hate groups. There are even instances of reprisals against operators of sites that provide health and nutrition information for women, reproductive rights information, etc.

5. **Journalists operating in hostile territory**

Journalists posting stories from hostile territories may have a need or wish to operate a website while maintaining the security and privacy surrounding their identities and address information, including that of their collaborators, translators, etc.

Exploration of Secure Credential Technologies

There are various secure credentials on the market, such as Microsoft's U-Prove (http://research.microsoft.com/en-us/projects/u-prove/) and IBM's Identity Mixer (http://researcher.watson.ibm.com/researcher/view_project.php?id=664). These approaches permit the recipient to prove various attributes---such as that he or she has been recognized and authenticated by a trusted authority, that they have paid for a certain right or service----without revealing any personal information about themselves or providing any trace-back to the transactions which enabled the attributes. Relying parties have secure cryptographic proof that the entity being issued secure credentials has the trusted authority's approval, without needing to know who they are or how they got that approval.

Such technology could be used to establish a process whereby at-risk entities described above could get a domain name that has been registered using a secure protected credential. Neither the Registrar nor the Validator would have information about who the at-risk entities are beyond the requisite contacts responsible for dealing with DNS issues. They would therefore legitimately not be able to respond to requests for personal or address information. Obviously, there are concerns about technical compliance, abuse and the mitigations of these risks (discussed below). The key point is that for domain names registered using secure credentials, Registrars and Registries will no longer be the bearers of the risk and responsibility of identification of vulnerable individuals to their aggressors.

Operational Issues

In order to unpack the issues and risks associated with such a service, the EWG explored the following potential situations:

1. An information requestor wishes to establish the true name or address of an individual as described in 2, 3, & 4 above, for what they represent as legitimate purposes (allegations of trademark abuse, desire to buy or sell a domain name, wish to investigate product safety, etc.). Note that in a life and death situation, a Registrar is in a difficult position when trying to determine whether the requestor is acting under false pretenses, and staff cannot be

expected to understand what kind of unknown threats people may face, particularly in cases of identity change.

2. A requestor approaches the domain name's Registrar (or a designated PBC's Validator) alleging some kind of criminal or libelous activity and demands take-down of a website using that domain name. In these situations, the Registrar and Proxy Service Provider's terms of service would be followed, possibly leading to a reveal request to obtain the domain name licensee's identity and address. However, for domain names registered using secure credentials, a successful reveal leads only to the trusted authority that approved the secure credential. At this point, the trusted authority would be responsible for investigating potential DNS abuse. In some instances, such as criminal activity, expedited take-down may be granted for these websites.

3. In cases where government agencies make allegations of political speech rising to the level of treason or other criminal matters, Registrars may still be forced to use expedited take-down for websites using domain names registered with secure credentials, depending on the relevant law in the jurisdiction.

Even given these limitations, secure credentials would provide much more security to at-risk entities than they currently enjoy, and if the new RDS will require enhanced data accuracy and accountability, then a service such as this is required. To accomplish this, the following key functions would need to be developed:

1. A process to establish criteria for at-risk entity eligibility for secure credentials, starting with the user examples cited above and any others which the ICANN community deems appropriate through policy development.

2. Application forms, required attestations, and financial systems, all with a focus on ensuring that the identities of the at-risk entities (and, in some cases, their attestors) are protected. In any anonymous system, this is one of the key weak points.

3. An independent review board to evaluate and approve applications for secure credentials and the attestations of trusted parties, such as governments who have authorized name changes, United Nations organizations engaged in the protection of refugees, international associations of journalists, etc.

4. Trusted parties (such as those listed in #3 above) willing to relay secure credential applications and resulting domain names to/from this

independent review board. These trusted parties – referred to hereafter as Secure Credential Recipients – must attest to the at-risk entity's need for anonymity and accept accountability for any potential DNS abuse by secure credential-registered domain names.

5. Accredited proxy service providers that would be willing to accept secure credentials when registering domain names to be licensed by the Secure Credential Approver, along with the financial systems whereby they would be paid.

6. Policies surrounding expedited take-down procedures and other mitigations of DNS abuse. This might include enhanced security monitoring of secure credential registered domain names, to mitigate against potential DNS misuse and abuse and to help protect the domain names from attacks. Parties alleging DNS abuse would make their case to the board that approved the at-risk entity's application; that Secure Credential Approver would evaluate alleged abuse.

The following figure illustrates possible relationships between these parties, their responsibilities, and the flow of communication among them.

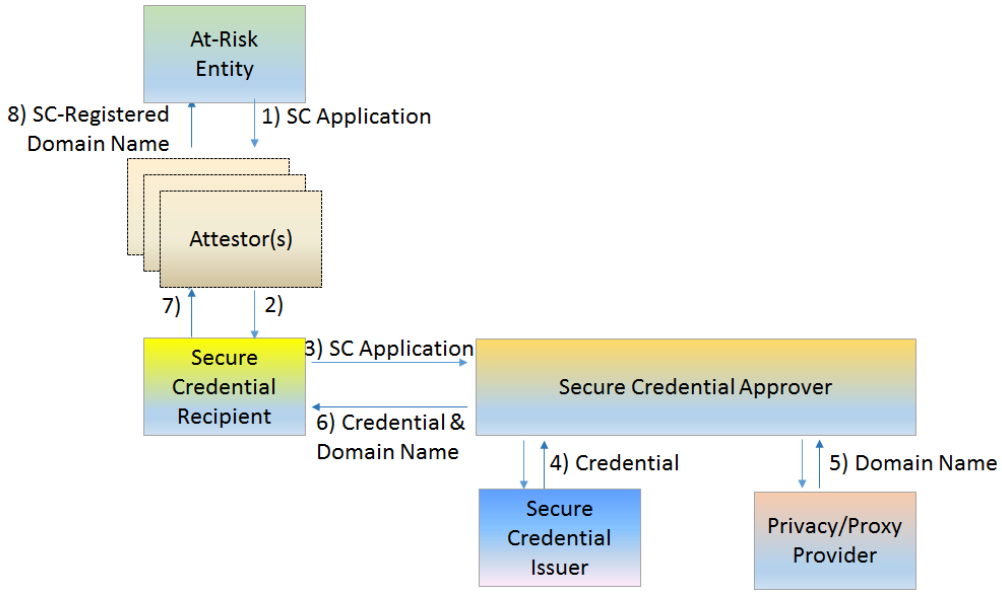


Figure 8. Secure Protected Credentials Model

Residual Risks

Secure credentials are not in widespread use because, among other reasons, they are complex to implement, particularly with respect to registration and revocation. It has been argued that all parties ought to be eligible for such registration, but given the work threshold required to establish this service and ensure that it is not used for fraudulent or criminal purposes, the EWG considers this approach unfeasible. The EWG recommends that Secure Protected Credentials be developed for limited use and after ensuring entities availing themselves of the service do indeed have legitimate need for anonymity.

It is also recognized that once such a domain name is registered and the website using it is operational, various kinds of Internet traffic metadata and content may lead to the identification of the domain name user. This is beyond the scope of ICANN's concern, which is solely focused on the domain registration issues and the attendant data that is collected, used and disclosed to meet defined purposes within ICANN's remit. Information generated from the actual use of a domain name must be the responsibility of the entities applying for and using secure credential-registered domain names, and it may be important to provide information underscoring this risk. ICANN's responsibility ends with the domain name system itself.

No.	Principles for Secure Protected Credentials
150.	Individuals and groups who can demonstrate that they would be at risk if identified must be able to anonymously apply for and receive domain names registered using secure credentials, aided by attestors and trusted third parties to provide a shield between at-risk entities and Registrars/Validators.
151.	ICANN must facilitate the establishment of an independent trusted review board that will validate claims of at-risk organizations or individuals to approve (and when necessary, revoke) credentials. Such an organization – referred to herein as a Secure Credential Approver (SCA) -- might develop other services, such as educating users about risks and safe Internet practices.
152.	ICANN must facilitate the development or licensing of a Secure Credential Issuer that recognizes SCA approvals and generates corresponding Secure Credentials.
153.	The Secure Credential Approver must use issued Secure Credentials to license domain names from accredited Proxy Service Providers in the usual manner.

No.	Principles for Secure Protected Credentials
	Information of the proxy service provider will appear in the RDS. No data about the at-risk entity using the secure credential-registered domain name would be known to the RDS, and some system of anonymous or proxy payment would have to be used.
154.	Domain names registered using secure protected credentials must follow regular accredited Privacy/Proxy service provider reveal and take-down procedures. Failure of the Privacy/Proxy customer (i.e., the Secure Credential Approver) to respond in a timely manner, or evidence of DNS abuse, could result in expedited take-down of secure credential-registered domain names.
155.	Recognizing that domain names registered using secure protected credentials might be at risk themselves for cyberattack, or that investigation of offences would be difficult, heightened security monitoring of these domain names could be considered to mitigate risk.
156.	Policies and processes must be established for secure protected credential application approval and revocation. • The approval process must allow for zero or more attestors to sufficiently shield the at-risk entity's identity and location from the trusted Secure Credential Recipient that presents the application to the SCA. The number and identity of attestors is transparent to the RDS; the only party that directly interfaces with the SCA is the Secure Credential Recipient. • The revocation process must allow for similar shielding of the at-risk individual's identity and location while enforcing secure credential terms of service. The SCA must be accountable for investigating alleged DNS abuses involving secure credentials and enforcing Terms of Service. In the case of DNS abuse severe enough to warrant credential revocation, the SCA shall hold the Secure Credential Recipient accountable.

c. Summary of Privacy Key Benefits

With improvements in accuracy and accountability, it will become even more important to protect individual citizens, particularly the vulnerable. Incorporating data protection, accredited Privacy/Proxy, and Secure Protected Credential principles and mechanisms as an integral part of the next- generation RDS will improve the privacy of Registrants and Contacts.

The EWG's recommended data protection principles would:

- More uniformly protect personal data by applying a single harmonized RDS policy, implemented consistently throughout the RDS ecosystem and using a "rules engine" to apply local law.
- Require less registration and contact data to be public and anonymously available.
- Better protect Registrant and Contact data against misuse.

The EWG's recommended principles for accredited Privacy/Proxy providers would:

- Provide greater clarity for Registrants seeking Privacy/Proxy services by establishing an accreditation framework for providers that offer such services.
- Require identification of the domain name as having been registered using services offered by an accredited Privacy/Proxy provider.
- Clearly indicate within registration data how to contact that Privacy/Proxy provider.
- Prevent third parties from using accredited Privacy/Proxy provider contact data without authorization.
- Require an accredited Privacy/Proxy provider to relay email to the underlying Registrant and respond to inquiries.
- Provide more consistent and predictable expectations to law enforcement and other third-party abuse reporters and reveal requestors.

The EWG's recommended Secure Protected Credential principles would:

- For the first time, establish procedures for the enablement of vulnerable and disadvantaged groups to benefit from the many advantages of holding their own domains on the Internet.
- Safeguard those who most need to use the Internet for the purposes of free speech and communication within groups, while providing remedies for potential abuse.
- Remove a potential liability from Validators and Registrars, who today bear the responsibility for revealing highly sensitive personal information through social engineering attempts.
- Provide additional security surrounding domain names registered using Secure Protected Credentials.
- Require expedited take-down of Secure Protected Credential-registered websites engaged in DNS misuse.

VIII. Possible RDS Models

a. Model Design Principles

This report provides details about several alternative models explored by the EWG, along with analysis of how these models might satisfy the EWG's recommended principles. All models were evaluated using a set of multi-faceted criteria as identified in Annex F.

In conducting its analysis, the EWG applied the following design principles:

No.	Model Design Principles
157.	**Collection:** Today, Registrars or Registrar's Affiliates collect and store registration information from their own customers (Registrants). This process is inherently distributed. In addition to continuing to collect registration data from Registrants by Registrars or Affiliates, the EWG proposes collection of contact data by Validators.
158.	**Storage:** Multiple possible models exist for storing registration information across all gTLDs. The EWG identified several possible models, pinpointed two that appeared to be most promising, and chose one recommended model by applying the evaluation criteria reflected in Annex F**.**
159.	**Access:** To protect data subject privacy, a centralized interface must enable appropriate requestors to access registration information across all gTLDs, including unauthenticated public data access by anyone and authenticated gated data access by accredited users.
160.	**Protocol:** The RDS must use RDAP[33] or EPP (as appropriate for each interface) as the underlying directory access protocol to obtain registration information from storage locations, wherever that may be.

[33] http://tools.ietf.org/html/draft-ietf-weirds-rdap-query-02

b. Models Considered

In order to test the alternative system models considered by the EWG in its Initial Report and additional models suggested by the ICANN Community, the EWG first determined which models should be examined in depth. Each of the models differs in a variety of ways, including how registration information is copied to or queried through the RDS. These differences are summarized in the table below[34] and further explained in Annex F.

POSSIBLE MODELS	Collection	Storage	Copy	Access
Current WHOIS	RR	RR/Ry	n/a	RR/Ry
Federated	RR & V	RR/Ry & V	n/a	RDS
Synchronized *	RR & V	RR/Ry & V	RDS	RDS
Regional	RR & V	RR/Ry & V	Regional	RDS
Opt-Out	RR & V	RR/Ry & V	Optional	RDS
Bypass	RR & V	RR & V	RDS	RDS

* **Note:** The model previously referred to as the **"Aggregated RDS (ARDS)"** has been re-named the **"Synchronized RDS (SRDS)"** to better reflect that model's property of using data that resides in multiple places in a consistent, coordinated way. ALL models considered here would be deployed using engineering best practices to achieve fault tolerance, high availability, and load balancing, including geographically-diverse data centers, robust diverse connectivity, and redundant infrastructure at each data center.

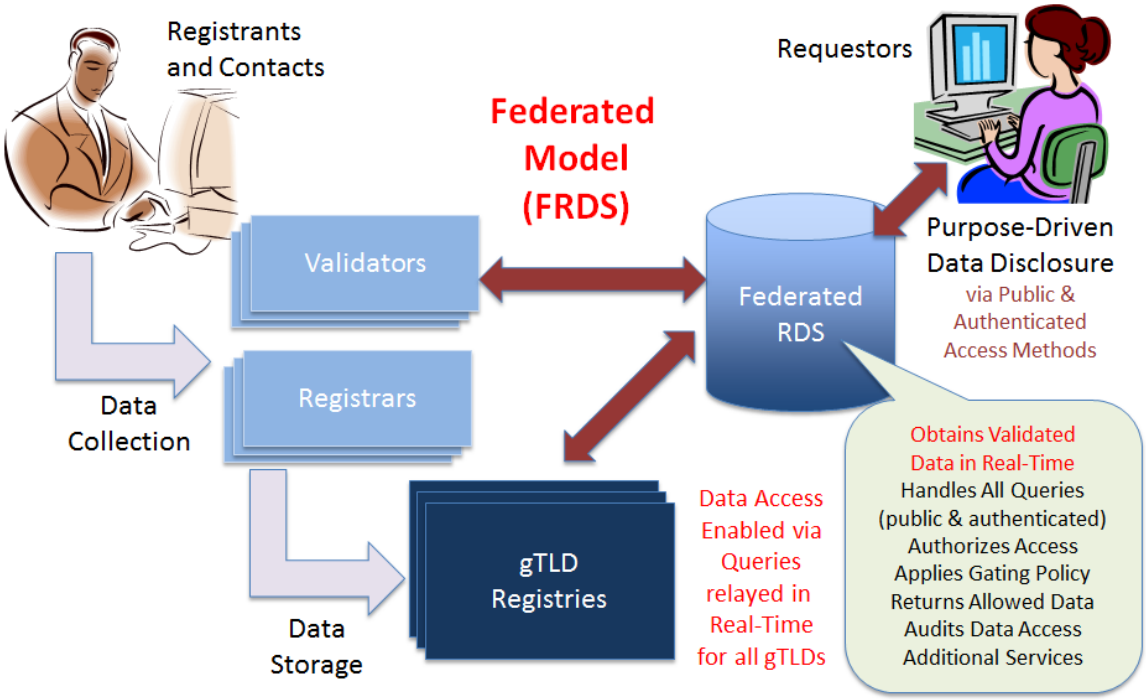
c. Recommended Model

Of the possible system models identified above, each differs in the way that registration information is copied to or queried through the RDS. The EWG closely examined each to determine how these differences might impact various attributes. After comparing these possible models, the EWG found that except for the current WHOIS, all are capable of satisfying the EWG's recommended RDS principles to some degree. Of these, the EWG focused on the two most promising models for further examination –the Federated Model and the Synchronized Model (formerly known as the "Aggregated Model") –**and ultimately recommended the Synchronized Model (SRDS).**

[34] Key for Model Overview Table: RR refers to Registrars, Ry refers to Registries, V refers to Validators

Federated Model (Runner-up)

This model describes an RDS that pulls registration information from distributed storage areas operated by thick Registries and Validators, which all use a common federated data schema. There is no aggregation of data into a single storage location, but rather unified public/gated access through the RDS to registration information obtained in real-time from all gTLD Registries (domain name data) and Validators (contact details).



In this model, data is pulled by the FRDS from Validators and Registrars/Registries via RDAP. The flow of contact and registration data associated with this model is further detailed in Annex I (RDS Process Flow Charts) and illustrated in Annex E using example queries.

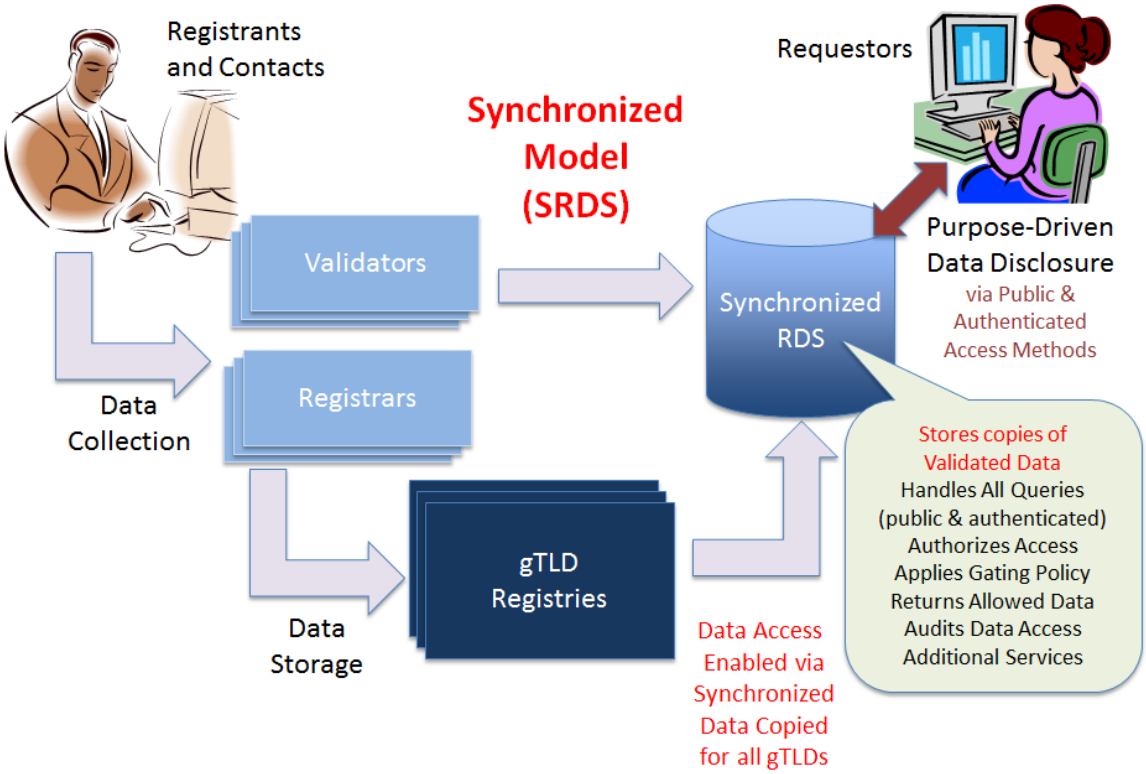
Synchronized Model (SRDS) (Recommended)

This model describes an RDS that, in near real-time, copies data received from distributed storage areas operated by thick Registries and Validators into a synchronized system that aggregates and stores data in a distributed architecture operated by the RDS.

Under this model, the RDS is the authoritative data source and provides authoritative access, as described. As a result, the RDS would move beyond the current RAA requirement (and current need) for Registrar and Registry timeliness of updates. Registries, Registrars and Validators can provide customers with access to their own data, but all requests for gated data must be answered by querying the RDS. This model

is responsive to previous WHOIS recommendations and requests to reduce consumer confusion as to where and how to access registration data, and also minimizes cost and accountability requirements for Registrars and Registries.

Although the RDS provides access to the data, the data is not stored in a single location but instead in multiple locations, diversified and redundant per engineering best practices for systems that require fault tolerance, high availability, and load balancing. Registries and Validators continue to store their own data, but the RDS can use synchronized copies of that data to process access requests more effectively.



In this model, data is pushed to the SRDS by Validators and Registrars/Registries via EPP. The flow of contact and registration data associated with this model is further detailed in Annex I (RDS Process Flow Charts) and illustrated in Annex E using example queries. Described below is a relative comparison of these two EWG-preferred models, after applying the methodology identified in Annex F.

- **Security Implications**- Both of these models produce similar results when evaluated against their impact on security. Although there were public comments that an Aggregated (subsequently renamed Synchronized) model such as suggested in the Initial Report posed a risk due to a "single point of failure" from a centralized interface, the EWG found that was not dissimilar to risks posed today by large gTLD Registries and global-scale Internet websites. Current best practices dictate that

large information-based systems utilize multiple data centers, back-up storage and disaster recovery systems, as well as a geographically diversified and fully redundant infrastructure in order to mitigate these risks.

A Synchronized Model has the added benefit of being better able to ensure consistent security implementation and policy enforcement. By tightly operating components of the system, a synchronized model with distributed architecture that is managed by one operator would likely produce a more uniform approach to reaching stated security goals as compared to the Federated Model. This is in part because in a Federated Model, potentially thousands of Registries, Registrars, and Validators would manage their respective databases, with differing levels of Registrar/Registry/Validator expertise and investment in security practices.

- **Jurisdictional and Privacy Concerns –** Both of these models produce similar results when evaluating the jurisdictional and privacy impacts. In the Federated Model, the data is stored and controlled at the Registry level with additional copies retained in other locations (namely, that of a Registrar, Validator, and back-up data centers located throughout the world).The Synchronized Model stores and controls the data in multiple locations separate from Registries, with additional copies retained in other locations (Registrar, Registry, Validator, and back-up data centers located throughout the world). When looking at all of the models evaluated, most did not eliminate the transfer of data to multiple locations, except for the “bypass model,” which eliminates the need for Registries to store the contact data.

  Moreover, the Synchronized Model enables a more consistent application of rules to conform to local privacy requirements, as it is easier to manage rules administered by one entity (the operator of the Synchronized RDS) rather than by the potentially thousand-plus participants in a Federated Model.

- **Accreditation –** The application of accreditation requirements is possible in both Synchronized and Federated models. Both models can offer features to track and enforce abusers of the accreditation system, although it may be easier to do this when the database is managed by one entity in a Synchronized Model, as compared with the potentially thousand-plus participants in the Federated Model. Further, implementation of a Federated Model would require added expense as well as detailed contractual obligations, service level agreements, and ICANN compliance oversight to support consistent enforcement and auditing capabilities.

- **Operation –** The Synchronized Model offers efficiencies in some operational areas that are more difficult to achieve in a Federated Model. For example, deploying a user-friendly portal that displays data in multiple languages/scripts might be easier in the Synchronized Model, where contact data could be translated or transliterated in a more consistent format. To achieve similar consistency in a Federated Model, the agreements would need clearly articulated translation/transliteration standards specifications. Both models can be designed to allow random data quality audits, although this is likely easier to accomplish within a Synchronized Model.

  Data latency and synchronization concerns are reduced in a Federated Model, since the data to be displayed comes directly from the Registry itself. However, pulling data from a Synchronized Model introduces latency issues that can be overcome by having Validators and Registrars (via Registries) push timely EPP updates to the SRDS (see compliance principle #108).

- **Implementation –** A Federated Model is more closely aligned to the distributed model of today's WHOIS, than is a Synchronized Model. However, the performance requirements and search capabilities necessary to provide the robust features recommended by the EWG would require detailed specifications and performance metrics that far exceed those offered in today's WHOIS. Greater ICANN compliance oversight and resources would be needed to ensure that all parties in the Federated system perform at the expected level. Under either model, the affected participants would need to update their software platform to interact with the RDS interface to deliver the search results and contact data required.

- **Costs –** There may be cost savings realized by Registrars and Registries (and also Validators) under the Synchronized model by being relieved of the operational burden of constantly responding to complex queries from the RDS interface (such as Reverse Queries) as would be required under a Federated system. In particular, the model cost comparison (further detailed in Annex F) reached the following conclusions:

  (1) With the assumptions used, the Core RDS system is slightly less expensive in the Federated RDS (FRDS) model than the Synchronized RDS (SRDS) model. However, the Federated model is highly sensitive to the number of Reverse Queries. **With a higher amount of Reverse Queries, the FRDS model becomes substantially more expensive than the SRDS.** For example, with a 3% Reverse Query load instead of a 1% Reverse Query load, the cost of the FRDS model becomes 35% more expensive than the SRDS model. With 5% Reverse Queries,

the global FRDS cost is expected to increase about 85%. This is an important factor of uncertainty and risk associated with the FRDS model. The SRDS model is believed to be less sensitive to the amount of Reverse Queries.

(2) In addition, **the FRDS model has a higher cost on the entire ecosystem because [of its higher cost] impact on the Registry Operators**. In the FRDS model, each Registry Operator would have to implement and support – pursuant to SLA's – responses to RDS RDAP queries in real-time, including Reverse Queries and historical WhoWas Queries. For the latter, historical data would also have to be maintained by the Registry Operators, further increasing cost to Registries. Note that this additional per-Registry cost would be above and beyond the above-estimated core RDS system impact.

(3) Furthermore, **the FDRS model would require higher application operations, support, maintenance and test efforts** as compared to the SRDS model, since greater interactions with Registry Operators are expected.

More details about this model cost analysis, its scope and methodology, and the underlying volumetrics and assumptions, can be found in Annex F and "*Registration Directory Service (RDS) Implementation Model Cost Analysis*[35]" prepared for ICANN by IBM in March, 2014.

d. Data Storage, Escrow, and Logging Principles

No.	Common Requirements for Storage, Escrow, and Logging
161.	Location, retention, privacy, and access policies must be developed.
162.	Storage, escrow, and logging policies and implementations must comply with local and international laws.
	Storage Principles
163.	To maintain redundant systems and eliminate the single point of failure, the data must reside at multiple locations (i.e., Validator, Registrar, Registry, Escrow Provider, and RDS Provider).
164.	Consistency must be maintained when data exists in multiple places.
165.	The RDS must maintain the data elements in a secure fashion, protecting the confidentiality and integrity of the data elements that are at risk from

[35] https://community.icann.org/display/WG/EWG+Public+Research+Page

	unauthorized disclosure or use.
166.	Transaction data must be stored indefinitely to maintain an accurate record of data changes over time and support WhoWas functionality, but no longer than limits (if any) required for compliance with applicable data protection laws. Orphaned contact information should also be purged periodically, in accordance with laws (e.g., one year after disassociation).
	Escrow[36] Principles
167.	Audits must be conducted of escrow data to test the format, integrity, and completeness of deposits.
168.	Escrow and audit of escrow may be easier to coordinate with a synchronized RDS model.
169.	Escrow data itself must be encrypted and opaque to auditors.
170.	Escrow data must be retained for a period of time that is consistent with the requirements of the Registrar Accreditation Agreement, individual gTLD Registry Agreements, and applicable data protection laws. Currently, this would be for the duration of the publishing entity's sponsorship of the data and for a period of two additional years thereafter or longer if required by the gTLD Registry Agreement, but no longer than the maximum allowed by law.
	Logging Principles
171.	RDS queries must be logged to provide records of how the system is used.
172.	Log aggregation may be needed to detect abuse directed at distributed systems.
173.	Changes must be logged to provide data element history over time.
174.	Access to operational RDS logs must be restricted to those trusted, authenticated, authorized individuals and entities with a specific purpose and "need to know." This must include authorized operators of the RDS itself (to confirm and trouble-shoot proper RDS operation) and authorized data protection entities (to monitor RDS compliance with data protection legislation.) (See also Section VIII(b), Law Enforcement Access.)

[36] Escrow refers to encrypted system backup to a trusted third party (Escrow Provider) for purposes of recovery in the event of disaster, system failure, etc. Refer to the RAA for further details.

IX. Costs and Impacts

a. Cost Principles

As noted in Annex F, Methodology for Model Comparison, the EWG also considered RDS costs and impacts. The EWG acknowledges that some aspects of the recommended model will incur new costs, but believes that many other hidden costs incurred with today's inefficient and too-often-inaccurate WHOIS system will be reduced. As the recommended RDS delivers new and improved services, both benefits and costs must be evaluated. The recommended approach will provide policy-makers the option, for the first time, to craft ways for those requesting registration data from the system to efficiently contribute to the operation of that system.

The costs of operating WHOIS are unknown today, but include costs to the entire ecosystem, not just to the Registries and Registrars who offer the WHOIS services. Registrars are not required to break out WHOIS costs, and may have difficulties distinguishing between the costs of providing such services for gTLDs versus ccTLDs. Other players in the ecosystem incur costs as a result of the inefficiencies and deficiencies in today's WHOIS, such as trademark holders who pay for the services of brand protection companies and commercial WHOIS services to identify cybersquatters.

The EWG recommends the following cost principles:

No.	Cost Principles
175.	Unauthenticated (non-gated) access to public data elements must be free.
176.	Authenticated (gated) access by law enforcement to authorized data elements (subject to due process) may be subject to special cost consideration.
177.	RDS design should strive for cost-efficiency and minimization, without compromising other goals.
178.	RDS should operate on a cost-recovery model.
179.	To facilitate migration from WHOIS, an RDS software development platform should be created and funded by ICANN to minimize RDS implementation costs on Registrars/Registries, Validators and RDS User Accreditors.
180.	Provision of this software development platform should not be unduly burdensome on other RDS users.

Without delving into specific implementation details, costs could be shared throughout the ecosystem. Examples of where costs could be recovered include imposing varying licensing fees, depending upon the user, data elements accessed, or the purpose (such as commercial use fees, subscription fees for power users, or premium access fees), or charging fees for related services (such as credentialing fees or pre-validation fees).

The RDS may also produce cost savings for Registries and Registrars who are no longer required to provide public access or meet stringent service level response times. Cost savings may also be realized for requesters seeking data by eliminating inefficiencies due to non-compliant providers (Registrars, Registries, Validators, or accredited Privacy/Proxy service providers).

b. Benefits compared to Current WHOIS under the 2013 RAA

WHOIS deficiencies have been documented over the last decade by numerous reports and studies, highlighted in Annex B. Improvements to WHOIS, as reflected in the new 2013 Registrar Accreditation Agreement (2013 RAA), coupled with the other improvements resulting from the ICANN Board's evaluation of the WHOIS Review Team Recommendations, have addressed some perceived deficiencies in WHOIS.

Although the 2013 RAA introduced several new obligations, most notably validation and verification requirements to improve accuracy, there are other significant deficiencies that continue to exist. These deficiencies are summarized below, mapped to sections of this report that contain recommendations to achieve further benefits.

WHOIS under the 2013 RAA Deficiency	Addressed by RDS in Section
Anonymous public access of all data elements creates an environment where mining & abuse can occur, with little accountability or ability to remedy	III Users/Purposes IV Improving Accountability VI(d) Accountability and Audit
Limited ability to protect the privacy of individuals	VI(a) Data Protection VII Improving Registrant Privacy
Limited ability to ensure integrity of registration data; Registrants can easily insert false contact details, including those held by another	V Improving Data Quality V(g) Unique Contact Data Capability
Lack of Security Features	IV(b) Unauthenticated and Gated Data Access IV(c) RDS User Accreditation
Lack of auditing capabilities	VI(d) Accountability and Audit

WHOIS under the 2013 RAA Deficiency	Addressed by RDS in Section
	VIII(d) Data Storage, Escrow, and Logging
Access not directly linked to stated legitimate purposes	III Users/Purposes III(e) Purpose-Based Contacts
Inconsistent WHOIS query interfaces and responses	IV(b) Unauthenticated and Gated Data Access VIII Possible RDS Models
No support or standards for displaying internationalized registration data	IV(b) Unauthenticated and Gated Data Access V(e) Interaction with Validators
Limited ability to apply different rules to conform to differing data privacy regimes	VI(a) Data Protection
Unacceptable accuracy levels creates inefficiencies for those seeking to communicate with Registrants	V Improving Data Quality III(e) Purpose-Based Contacts
Cumbersome management processes to update contacts across multiple domain names	V Improving Data Quality V(c) Accuracy, Audit, and Remediation Process
Difficulties in identifying and communicating with the customers of privacy and proxy services	III(e) Purpose-Based Contacts VII(a) Privacy/Proxy Services Annex H Relay and Reveal Model
No regulation of privacy or proxy services, beyond 2013 RAA requirements that apply only to Registrars and their affiliates	VII(a) Privacy/Proxy Services Annex H Relay and Reveal Model

c. Risks and Impact Assessment

As noted in Section IV, Improving Accountability, the EWG recommends performing a widely scoped risk assessment to confirm that the RDS principles recommended herein do in fact result in appropriate collection and disclosure of data for defined purposes, striking the right balance between risks and benefits.

On March 14, the EWG invited all parties that provide or use gTLD domain name registration data to participate in an on-line RDS Risk Survey,

including Registrants, Registrars, Registries, and the broad spectrum of individuals, businesses, and other organizations that consume WHOIS data today. This survey offered respondents a chance to tell the EWG about the risks and benefits that a next-generation WHOIS replacement system might have for them.

Before finalizing this report, the EWG examined a snapshot of the risks and benefits identified through this survey in hopes of and reducing unanticipated and unnecessary risks. Through 29 May, 2014, the English version of this survey had garnered 180 partial responses; roughly 100 had completed the entire survey. Respondents to date came from North America (68%), Europe (35%), Asia (20%), Latin America (14%), Africa (11%), and Oceania (10%) and were evenly divided between those who USE and PROVIDE registration data. Responses shed light on the most likely and impactful risks and benefits in the following areas: technical, operational, legal and financial, security and privacy. About two dozen respondents also commented on unavoidable and acceptable risks and on ways to shift or reduce risk.

To enable broad community input on this topic, the EWG has decided to leave the RDS Risk Survey open through July 2014 and launch translated versions. Responses will be used to inform the ICANN Board's review of this report and as input to a future formal analysis of costs, risks and benefits for all stakeholders that would be impacted by replacement of WHOIS with the RDS[37].

[37] See also ICANN's DNS Risk Assessment (1st Iteration) for Public Consultation

X. Conclusion and Next Steps

After considering the perspectives of the many stakeholders in the ecosystem who rely on registration data, the EWG unanimously recommends abandoning today's WHOIS model – giving every user the same anonymous public access to gTLD registration data – with a replacement system, built from the ground up.

The EWG believes that the principles and the next-generation RDS recommended in this Final Report provide a more solid foundation than exists today – a foundation from which to protect personal privacy and ensure greater accuracy, accountability, and transparency for the entire ICANN ecosystem for years to come. The RDS builds upon, but goes well beyond, the improvements made under the recently negotiated 2013 RAA, as described more fully in the Section IX(b).

While the Final Report may appear to some as overly detailed, it is not comprehensive. As noted in Annex A, the report addresses each of the questions posed by the Board. However, several issues remain to be more fully addressed in the future – either in any follow-on policy development process (PDP) or any related implementation efforts.

- **Accreditation Bodies and policies for RDS user communities.** As specific user communities may have access to gated data for an approved purpose, policies for identifying who qualifies as members of that community should be examined during the implementation phase, as should possible Accreditation Bodies and models appropriate for each community.
- **Extensions required to EPP and RDAP.** As detailed in Annex G, the EWG recommends that standards protocols be used to support RDS needs, but has identified certain extensions that would be required to fully support the recommended RDS model and data elements.
- **Risk and Impact Assessment.** As discussed in Section IX, the EWG recommends that a full risk assessment and cost/benefit analysis be undertaken prior to implementation of the recommended RDS, and already launched a survey to gather input to that process.
- **RDS privacy policy.** As discussed in Section VII, the EWG recommends that a basic ICANN privacy policy for the RDS be drafted based on standard best practices for privacy protection, and standard contractual clauses be developed which give effect to this policy throughout the RDS ecosystem.
- **Translation/transliteration of contact data.** As there is a policy development process (PDP) currently underway on this issue, the EWG chose not to duplicate efforts beyond the principles identified in Section IV(b), and instead suggests that

the outcome of the current PDP may be examined in the future to determine how to apply any new policies to the RDS.

- **Privacy and Proxy Services.** The EWG's principles related to accredited Privacy/Proxy Providers will need to be considered in combination with the work currently underway in the GNSO on this topic, reconciling the outcome of the current PDP with any implementation of the RDS.
- **Validator Ecosystem.** The creation of an accreditation program for Validators, and the processes used to validate contact details for Registrants and Contacts located throughout the world, needs further exploration during the implementation phase.

The RDS reflects carefully crafted and balanced compromises with interdependent elements that should not be separated. These compromises are informed by the input received by the EWG in the many public comments, webinars and consultations received on its work to date. As a result, the EWG encourages the Board to forward the Final Report to the GNSO for adoption as a whole. Choosing to adopt some but not all of these RDS design principles undermines the intended benefits for the entire ecosystem. The EWG is concerned that examining the components individually may lead to a repeat of the dissention and stalemate in the Community that has accompanied past attempts at improving WHOIS.

The EWG has delivered this Final Report to ICANN's CEO and Board, publicly posted it online, and will hold multiple sessions at ICANN's June 2014 meeting in London. It will also conduct webinars and other opportunities to discuss the report and answer ICANN community questions about it. The Final Report is intended to serve as a foundation for the Board-requested GNSO Policy Development Process (PDP) for the provision of gTLD registration data and for contractual negotiations, as appropriate. As the Board and the ICANN community considers this Final Report, the EWG recommends that consideration be framed by the following questions:

- Is the RDS preferable to today's WHOIS?
- If not, does the ICANN community agree that the current WHOIS system should continue, and it can meet the needs of the evolving, global Internet?

The EWG is confident that this Final Report fulfills the ICANN Board's directive to help redefine the purpose and provision of gTLD registration data, and will provide a solid foundation to help the ICANN community (through the GNSO) create a new global policy for gTLD directory services.

ANNEX A: RESPONSE TO THE BOARD'S QUESTIONS

The Board resolution that directed the EWG's work included a series of specific questions to be answered as it conducted its analysis. This Annex references the sections of this Report that address the Board's concerns.

Board Questions & Guidance	Report Sections
EWG to redefine the purpose of: • collecting, • maintaining, and • providing access to gTLD registration data, and • consider safeguards for protecting data	Section III, Users and Purposes Section VI, Improving Accountability
Why are data collected?	Section III, Users and Purposes Section VI(a), Data Elements
What purpose will the data serve?	Annex D, Purposes and Data Needs
Who collects the data?	Section V, Improving Data Quality Annex I, RDS Process Flow Charts
Where is data stored and how long is it stored?	Section VIII, Possible RDS Models Section VIII(d), Data Storage
Where is data escrowed and how long is it escrowed?	Section VIII(d), Data Storage, Escrow, and Logging Principles
Who needs the data and why?	Section III, Users and Purposes
Who needs access to logs of access to data and why?	Section VI(d), Accountability and Audit Principles
Public access to details about domain name registration?	Section IV(b), Unauthenticated and Gated Data Access Section VI(a), Data Elements Section VII, Improving Registrant Privacy
Law enforcement access to details about a domain name registration?	Section III, Users and Purposes Section VI(b), Principles for Data Access by Law Enforcement
Intellectual property owner access to details about a domain name registration?	Section III, Users and Purposes
Security practitioner access to details about a domain name registration?	Section III, Users and Purposes
What value does the public realize with access to registration data?	Section II(b), Purpose Section III, Users and Purposes
Of all the registration data available, which does the public need access to?	Section VI(a), Data Elements
Is the WHOIS protocol the best choice for providing that access?	Section IV(b), Unauthenticated and Gated Data Access

Board Questions & Guidance	Report Sections
	Annex G, Ability of EPP and RDAP Protocols to support RDS
Security	
What comprises a legitimate law enforcement need?	Section III, Users and Purposes Section VI(b), Principles for Data Access by Law Enforcement
How is a law enforcement agent identified?	Section IV(c), RDS User Accreditation Principles Section VI(b), Principles for Data Access by Law Enforcement
What registration data and to what level of accuracy comprises the real identity of the responsible party?	Section V, Improving Data Quality Section VI(a), Data Elements Section VII(b), Secure Protected Credentials
What registration data and to what level of accuracy comprises valuable information to a law enforcement agent that is looking for the real identity of the responsible party?	Section III, Users and Purposes Annex D, Purposes and Data Needs
Is the WHOIS protocol the best choice for providing that?	Section IV(b), Unauthenticated and Gated Data Access Annex G, Ability of EPP and RDAP Protocols to support RDS
Intellectual Property Owners	
Is the desired domain name registration data access consistent with access that intellectual property owners have to similar types of data in other industries?	Section III, Users and Purposes Section IV(c), RDS User Accreditation Principles
How is an intellectual property owner identified?	Section IV(c), RDS User Accreditation Principles
Of all the registration data available, what does an intellectual property owner need access to?	Section III, Users and Purposes Annex D, Purposes and Data Needs
What registration data is appropriate to be made available?	Section VI(a), Data Elements
Is the WHOIS protocol the appropriate method for access?	Section IV(b), Unauthenticated and Gated Data Access Annex G, Ability of EPP and RDAP Protocols to support RDS

ANNEX B: STUDIES EVALUATING WHOIS DEFICIENCIES

- SSAC - SAC 051 Report
- SSAC - SAC 054 Report
- SSAC - SAC 055 Report
- GAC WHOIS Principles
- The WHOIS Policy Review Team Final Report
- Draft ICANN Procedure for Handling WHOIS Conflicts with Privacy Law
- Inventory of WHOIS Service Requirements - Final Report
- WHOIS Taskforce 2 Initial Report (2009)
- Final Task Force Report on WHOIS Services (2007)
- Study to Evaluate Solutions for the Submission and Display of Internationalized Contact Data
- GNSO Thick WHOIS Final Report
- Interim Report from the EWG on Internationalized Registration Data
- Review of the ICANN Procedure for Handling Whois Conflicts with Privacy Law
- GNSO WHOIS Studies including
    - Study of the Accuracy of WHOIS Registrant Contact Information
    - Study on the Prevalence of Domain Names Registered using a Privacy or Proxy Service among the Top 5 gTLDs
    - WHOIS Misuse Study
    - WHOIS Registrant Identification Study
    - WHOIS Privacy & Proxy Service Abuse Study
    - WHOIS Proxy/Privacy Reveal & Relay Feasibility Survey + Appendices

ANNEX C: EXAMPLE USE CASES

As described in Section III, the EWG analyzed actual use cases involving the current WHOIS system to identify users who want access to gTLD registration data, their purposes for doing so, and the stakeholders and data involved. A list of representative uses cases considered by the EWG is provided below.

Purpose	Example Use Cases
Domain Name Control	Domain Name Registration Account Creation
	Domain Name Data Modification Monitoring
	Domain Name Portfolio Management
	Domain Name Transfer Initiation
	Domain Name Deletions
	Domain Name DNS Updates
	Domain Name Renewals
	Domain Name Contact Validation
Personal Data Protection	Contact Privacy/Proxy Provider
	Contact Secure Credential Approver
Technical Issue Resolution	Contact with Domain Name Technical Staff
Domain Name Certification	Domain Name Certification Issuance
Individual Internet Use	Real World Contact
	Consumer Protection
Business Domain Name Purchase or Sale	Domain Name Brokered Sale
	Domain Name Trademark Clearance
	Domain Name Acquisition
	Domain Name Purchase Inquiry
	Domain Name Registration History
	Domain Names for Specified Registrant
Academic/Public Interest Domain Name Research	Domain Name Registration History
	Domain Names for Specified Contact
	Survey Domain Name Registrant or Designated Contact
Legal Actions	Domain Name User Contact
	Combat Fraudulent Use of Registrant Data
	Domain Name Registrant History
	Domain Names for Specified Contact

Purpose	Example Use Cases
Regulatory and Contractual Enforcement	Online Tax Investigation
	UDRP Proceedings
	RDS Ecosystem Contractual Compliance
Criminal Investigation & DNS Abuse Mitigation	Investigate Abusive Domain Name
	Investigate Offline Criminal Activity
	Domain Name Reputation Services
	Investigate Online Criminal Activity
	Abuse Contact for Compromised Domain Name
DNS Transparency	Public Registration Data Access
Malicious Internet Activities	Domain Name Hijack
	Malicious Domain Name Registration
	Registration Data Mining for Spam/Scams

Table 7. Example Use Cases

To illustrate the EWG's methodology, a single use case is given below. Refer to Section III for additional descriptions of each use case and associated RDS users and data needs.

Technical Issue Resolution – Contact with Domain Name Technical Staff

Goal/Scenario #1

A person experiences an operational or technical issue with a registered domain name. They want to know if there's someone they can contact to resolve the problem in real or near-real time, so they use the RDS to identify an appropriate person, role, or entity that possesses the ability to resolve the issue. An incomplete list of examples of technical issues includes email sending and delivery issues, DNS resolution issues, and web site functional issues.

Brief Format Use Case

Use Case: Identify a person, role, or entity that can help resolve a technical issue with a domain name.

Main Use Case: A person accesses the RDS to obtain contact information associated with registered domain names under a TLD or TLDs. The person submits a domain name to the RDS for processing. The RDS returns information associated with the domain name that identifies a person, role, or entity that can be contacted to resolve technical issues.

Casual Format Use Case

Title: Identify a person, role, or entity that can resolve a technical issue with a domain name.

Primary Actor: Person experiencing a technical issue with a registered domain name.

Other stakeholders: Operator of the RDS; person, role, or entity associated with the registered domain name who can resolve technical issues; Registrant (who may care to know about operational issues); Validator (who may have issued a Contact ID to the Technical contact); Registrar or hosting provider (who may be providing an operational service); accredited Privacy/Proxy service provider (who may assist in reaching the person, role, or entity associated

with the domain name who can resolve technical issues).

Scope: Interacting with RDS

Level: User Task

Data Elements: Data elements that allow communication in real or near-real time are the most useful in the context of this use case. These include an email address, an instant messaging address, a telephone number, and/or an indicator that identifies the preferred contact method specified by the Registrant. Section 4 of RFC 2142 describes recommendations for abuse@, noc@, and security@ email addresses to "provide recourse for customers, providers and others who are experiencing difficulties with the organization's Internet service," but it is important to note that the public nature of these addresses often makes them attractive to unsolicited bulk email senders.

Story: A person (requestor) experiencing a technical issue with a registered domain name accesses the RDS to obtain information about registered domain names under a TLD or TLDs. The RDS could be accessible via a website or some other electronic processing means.

The requestor submits a registered domain name to the system for processing.

The RDS processes the request and either reports error conditions or proceeds to query gTLD registration data to retrieve information associated with a person, role, or entity that has been previously identified as a resource to help resolve technical issues for this domain name.

The RDS returns either the registration data associated with the domain name or an error condition that was encountered while retrieving the data.

Figure 9. Example Use Case

ANNEX D: PURPOSES AND DATA NEEDS

The EWG analyzed use cases to identify users who want access to gTLD registration data, their purposes for doing so, and the stakeholders and data involved. The following table summarizes the RDS data elements recommended in Section IV and mapped to permissible purposes defined in Section III. Refer to Section IV for collection and disclosure recommendations for each data element.

Data Element	Purposes
Domain Name	All
DNS Servers	Domain Name Control Technical Issue Resolution Domain Name Certification Business Domain Name Purchase/Sale Academic/Public Interest DNS Research Regulatory/Contractual Enforcement Criminal Investigation/DNS Abuse Mitigation
Registrant Name and/or Organization Registrant Type Registrant Contact ID Registrant Contact Validation Status Registrant Contact Last Updated Timestamp	All
Registrant Company Identifier	Domain Name Control Domain Name Certification Individual Internet Use Business Domain Name Purchase/Sale Legal Actions Academic/Public Interest DNS Research Regulatory/Contractual Enforcement Criminal Investigation/DNS Abuse Mitigation DNS Transparency

Data Element	Purposes
Registrant Postal Address, including: Registrant Street Address Registrant City Registrant State/Province Registrant Postal Code Registrant Country	Domain Name Control Domain Name Certification Business Domain Name Purchase/Sale * Academic/Public Interest DNS Research* Legal Actions* Regulatory/Contractual Enforcement Criminal Investigation/DNS Abuse Mitigation
Registrant Phone + Ext Registrant Alt Phone + Ext	Domain Name Control Technical Issue Resolution Domain Name Certification Business Domain Name Purchase/Sale * Academic/Public Interest DNS Research* Legal Actions* Regulatory/Contractual Enforcement Criminal Investigation/DNS Abuse Mitigation
Registrant Email Address Registrant Alt Email	All
Registrant Fax + Ext	Domain Name Control Domain Name Certification Business Domain Name Purchase/Sale * Academic/Public Interest DNS Research* Legal Actions* Regulatory/Contractual Enforcement
New contact methods Registrants may opt to publish: Registrant SMS Registrant IM Registrant Social Media Registrant Alt Social Media Registrant Contact URL Registrant Abuse URL	Could be useful for every permissible purpose as an alternative to Registrant Email Address

Data Element	Purposes
Admin Contact ID Admin Contact Data Elements	Domain Name Control Domain Name Certification Business Domain Name Purchase/Sale Academic/Public Interest DNS Research DNS Transparency
Legal Contact ID Legal Contact Data Elements	Domain Name Control Domain Name Certification Academic/Public Interest DNS Research Legal Actions Regulatory/Contractual Enforcement DNS Transparency
Tech Contact ID Tech Contact Data Elements	Domain Name Control Technical Issue Resolution Domain Name Certification Academic/Public Interest DNS Research DNS Transparency
Abuse Contact ID Abuse Contact Data Elements	Domain Name Control Domain Name Certification Academic/Public Interest DNS Research Criminal Investigation/DNS Abuse Mitigation DNS Transparency
Privacy/Proxy Contact ID Privacy/Proxy Provider Contact Data Elements	Domain Name Control Personal Data Protection Domain Name Certification Academic/Public Interest DNS Research DNS Transparency
Business Contact ID Business Contact Data Elements	Domain Name Control Domain Name Certification Individual Internet Use Academic/Public Interest DNS Research DNS Transparency
DNSSEC Delegation	Domain Name Control Academic/Public Interest DNS Research

Data Element	Purposes
Registration Status Client Status (Registrar) Server Status (Registry)	Domain Name Control Business Domain Name Purchase/Sale Academic/Public Interest DNS Research Regulatory/Contractual Enforcement Criminal Investigation/DNS Abuse Mitigation
Registrar Reseller Registrar URL Registrar IANA Number Registrar Abuse Contact Email Address Registrar Abuse Contact Phone Number URL of Internic Complaint Site	Domain Name Control Business Domain Name Purchase/Sale Academic/Public Interest DNS Research Regulatory/Contractual Enforcement Criminal Investigation/DNS Abuse Mitigation DNS Transparency
Registrar Jurisdiction Registry Jurisdiction Registration Agreement Language	All
Original Registration Date	Domain Name Control Business Domain Name Purchase/Sale Academic/Public Interest DNS Research Regulatory/Contractual Enforcement
Creation Date Updated Date Registrar Expiration Date	Domain Name Control Business Domain Name Purchase/Sale Academic/Public Interest DNS Research Regulatory/Contractual Enforcement Criminal Investigation/DNS Abuse Mitigation

Note: Access to gated Registrant data elements sometimes needed by purposes marked with * above may involve need-to-know approval; see Section III for discussion of “Approved Gated Data.”

ANNEX E: ILLUSTRATIONS OF GATED & UNAUTHENTICATED ACCESS

The following registration data record extends the 2013 RAA WHOIS example to reflect recommended RDS principles for data collection and disclosure.

Grey elements are optional to collect; the rest are mandatory.
Bold-faced elements are always public; the rest may be gated, at the Registrant's or Contact Holder's choice.

Registration Status: x **DNSSEC Delegation: signedDelegation** **Client Status: DeleteProhibited, RenewProhibited, TransferProhibited** **Server Status: DeleteProhibited, RenewProhibited, TransferProhibited** **Registrar: EXAMPLE REGISTRAR LLC** **Reseller: EXAMPLE RESELLER** **Registrar Jurisdiction: EXAMPLE JURISDICTION** **Registry Jurisdiction: EXAMPLE JURISDICTION** **Registration Agreement Language: ENGLISH** **Creation Date: 2000-10-08T00:45:00Z** **Original Registration Date: 2000-10-08T00:45:00Z** **Registrar Registration Expiration Date: 2010-10-08T00:44:59Z** **Updated Date: 2009-05-29T20:13:00Z** **Registrar URL: http://www.example-registrar.tld** **Registrar IANA Number: 5555555** **Registrar Abuse Contact Email: email@registrar.tld** **Registrar Abuse Contact Phone: +1.1235551234** **URL of the Internic Complaint Site: http://wdprs.internic.net/**	Supplied by Registry or Registrar
Domain Name: EXAMPLE.TLD **Name Server: NS01.EXAMPLE-REGISTRAR.TLD** Registrant Name: EXAMPLE REGISTRANT **Registrant Type: LEGAL PERSON** **Registrant Contact ID: xxxx-xxxx** (issued by RDS-accredited Validator) **Registrant Contact Validation Status (from Validator)** **Registrant Contact Last Validated Timestamp (from Validator)** Registrant Organization: EXAMPLE ORGANIZATION Registrant Company Identifier: D-U-N-S #12345 (issued by Dunn and Bradstreet) **Registrant Email: EMAIL@EXAMPLE.TLD**	Collected from Registrant

Registrant Alt EMail: EXAMPLE@OTHERDN.TLD Registrant Street: 123 EXAMPLE STREET Registrant City: ANYTOWN Registrant State/Province: AP Registrant Postal Code: A1A1A1 **Registrant Country**: AA Registrant Phone: +1.5555551212 Registrant Phone Ext: 1234 Registrant Alt Phone: <cellnumber> Registrant Alt Phone Ext: 1234 Registrant Fax: +1.5555551213 Registrant Fax Ext: 4321 Registrant SMS: <textingnumber> Registrant IM: <IMhandle> Registrant Social Media: <SMhandle> Registrant Alt Social Media: <OtherSMhandle> Registrant Contact URL: <link to contact me form or instructions> Registrant Contact URL: <link to abuse report form or instructions>	
Administrator Contact ID: xxxx-xxxx **(followed by Admin PBC Contact Details*)**	Registrant must publish Purpose-Based Contacts for mandatory PBC types
Tech Contact ID: xxxx-xxxx **(followed by Tech PBC Contact Details*)**	
Legal Contact ID: xxxx-xxxx **(followed by Legal PBC Contact Details*)**	
Abuse Contact ID: xxxx-xxxx **(followed by Abuse PBC Contact Details*)**	
Business Contact ID: xxxx-xxxx (only if Registrant Type = Legal Person) (followed by Business PBC Contact Details*)	
Privacy/Proxy Contact ID: xxxx-xxxx (only if Registrant Type = Privacy/Proxy Provider) (followed by PP Provider PBC Contact Details*)	

Key: Grey elements are optionally/conditionally collected; the rest are mandatory. Bold-faced elements are always public; the rest may be gated, at the Registrant's or Contact Holder's choice. * PBC Data Elements not fully illustrated here.

Example #1: Unauthenticated Public query for purposes of technical issue resolution

1) User submits Unauthenticated RDS Query
(DN = MerchantZ.gtld, Purpose = Tech Issue Resolution, Data = All)

2) RDS evaluates Query:
No Authentication, because Query is Unauthenticated
No Authorization, so access to Public Data is Granted
Access is restricted to Public Data needed for Tech Issue Resolution --
that is, all requested Public Data for domain name PLUS Tech Contact

3) RDS retrieves requested data elements:
MerchantZ.gtld data is retrieved from RDS cache (Synchronized) or Registry (Federated) delivering only Public Data Elements defined for this purpose, including

Registrant Contact ID = 12345
Registrant Type = Legal Person
Registrant Organization = MerchantZ, Inc.[38]
Tech Contact ID = 67890

Tech Contact ID [67890] is retrieved from RDS cache or Validator, obtaining only Public Data Elements expressly published by this contact for this purpose, including

PBC ID = 67890

PBC Name= <*name of entity responsible for resolving technical issues for domain name MerchantZ.gtld*>

PBC Email Address= <*mandatory email address of entity responsible for resolving technical issues for domain name MerchantZ.gtld*>

PBC Alt Email Address= <*recommended alternative email address of entity responsible for resolving technical issues for this DN*>

PBC Phone Number = <*recommended phone number of entity responsible for resolving technical issues for this DN*>

PBC Contact_URL= <*recommended contact link published by entity responsible for resolving technical issues for this DN*>

<*any optional public data elements published by this entity*>

4) The RDS returns error condition or successful response to the user. For example:

[38] Registrant Organization is collected from Registrants that set Registrant Type to Legal Person or accredited Privacy/Proxy Provider; may be absent when Registrant Type defaults to Undeclared

Domain Name: MerchantZ.gtld *Registration Status: x* *Client Status: DeleteProhibited, RenewProhibited, TransferProhibited* *Server Status: DeleteProhibited, RenewProhibited, TransferProhibited* *Registrar: EXAMPLE REGISTRAR LLC* *Registrar Jurisdiction: EXAMPLE JURISDICTION* *Registry Jurisdiction: EXAMPLE JURISDICTION* *Registration Agreement Language: ENGLISH* *Creation Date: 2000-10-08T00:45:00Z* *Registrar Registration Expiration Date: 2010-10-08T00:44:59Z* *Updated Date: 2009-05-29T20:13:00Z* *Registrar URL: http://www.example-registrar.tld* *Registrar IANA Number: 5555555* *Registrar Abuse Contact Email: email@registrar.tld* *Registrar Abuse Contact Phone: +1.1235551234* *URL of the Internic Complaint Site:http://wdprs.internic.net/*
Name Server: NS01.EXAMPLE-REGISTRAR.TLD *Registrant Contact ID = 12345* *Registrant Type = Legal Person* *Registrant Organization = MerchantZ, Inc.* *Registrant Email = 12345@MerchantZ.gtld* *Registrant Contact Validation Status = Operationally-Validated* *Registrant Contact Last Validated Timestamp = x* *<Other Optional Public Data Elements published by Registrant for this DN>*
Tech Contact ID = 67890 *PBC ID = 67890* *PBC Validation Status = Operationally-Validated* *PBC Last Validated Timestamp = x* *PBC Name: EXAMPLE TECHNICIAN* *PBC Email = 67890@SuperbHostingServices.gtld* *PBC Alt Email = SuperbHostingServices@OtherDN.gtld* *PBC Phone Number =+1.1235567890* *PBC Contact_URL=TechSupport@SuperbHostingServices.gtld* *<Optional Public Data Elements published by this PBC>*

Example #2: Authenticated Gated query for purposes of technical issue resolution

1) User submits Authenticated RDS Query
(DN = PersonY.gtld, Purpose = Tech Issue Resolution, Data = All)

2) RDS evaluates Query:
   - If "A" is Authentic, Gated Query is Approved
   - If "A" is an Accredited ISP, Access to Purpose Tech Issue Resolution Granted
   - Access is restricted to Public+Gated Data needed for Tech Issue Resolution
   - Access is restricted to Public+Gated Data needed for Tech Issue Resolution -- that is, all requested Public+Gated Data for this purpose PLUS Tech Contact

3) RDS retrieves requested data elements:
PersonY.gtld data is retrieved from RDS cache (Synchronized) or Registry (Federated) obtaining Public + Gated Data Elements defined for this purpose, including:

Registrant Contact ID = 12345
Registrant Type = Undeclared
<any optional public or gated data elements published by this Registrant – for example, if Registrant chooses, his/her name>
Tech Contact ID = 67890[39]

Tech Contact ID [67890] is retrieved from RDS cache or Validator, obtaining Public + Gated Data Elements expressly published by this contact for this purpose, including

PBC ID = 67890

PBC Email Address = <*mandatory email address of entity responsible for resolving technical issues for domain name PersonY.gtld*>

PBC Alt Email Address = <*recommended alternative email address of entity responsible for resolving technical issues for this DN*>

PBC Phone Number = <*recommended phone number of entity responsible for resolving technical issues for this DN*>

PBC Contact_URL = <*recommended contact link published by entity responsible for resolving technical issues for this DN*>

<*any optional public or gated data elements published by this entity – for example, SMS Number*>

[39] If Registrant does not supply any Contact IDs during DN registration, Registrant should be informed that the Registrant's own addresses will be published as the primary PBC and given a chance to consent, to provide another primary PBC ID (for example, a Privacy Provider's Contact ID), or cancel registration.

4) The RDS returns error condition or successful response to the user. For example:

Domain Name: PersonY.gtld *Registration Status: x* *Client Status: DeleteProhibited, RenewProhibited, TransferProhibited* *Server Status: DeleteProhibited, RenewProhibited, TransferProhibited* *Registrar: EXAMPLE REGISTRAR LLC* *Registrar Jurisdiction: EXAMPLE JURISDICTION* *Registry Jurisdiction: EXAMPLE JURISDICTION* *Registration Agreement Language: ENGLISH* *Creation Date: 2000-10-08T00:45:00Z* *Registrar Registration Expiration Date: 2010-10-08T00:44:59Z* *Updated Date: 2009-05-29T20:13:00Z* *Registrar URL: http://www.example-registrar.tld* *Registrar IANA Number: 5555555* *Registrar Abuse Contact Email: email@registrar.tld* *Registrar Abuse Contact Phone: +1.1235551234* *URL of the Internic Complaint Site:http://wdprs.internic.net/*
Name Server: NS01.EXAMPLE-REGISTRAR.TLD *Registrant Contact ID = 12345* *Registrant Type = Undeclared* *Registrant Email = 12345@PersonY.gtld* *Registrant Contact Validation Status = Operationally-Validated* *Registrant Contact Last Validated Timestamp =x* *<Other Optional Public or Gated Data Elements published by Registrant for DN, such as Registrant Name or Registrant SMS or Registrant Contact_URL >*
Tech Contact ID = 67890 *PBC ID = 67890* *PBC Validation Status = Operationally-Validated* *PBC Last Validated Timestamp = x* *PBC Name: EXAMPLE TECHNICIAN* *PBC Email = 67890@SuperbHostingServices.gtld* *PBC Alt Email = SuperbHostingServices@OtherDN.gtld* *PBC Phone Number =+1.1235567890* *PBC Contact_URL=TechSupport@SuperbHostingServices.gtld* *<Optional Public or Gated Data Elements published by this PBC>*

Example #3: Approved Gated Data queries for purposes of Domain Name Purchase/Sale or Legal Action

Investigation of possible trademark infringement is illustrated below, but similar starting points and steps apply to domain name purchase, merger/acquisition, and many other investigations within these and other purposes.

Step 1) The RDS User logs into an Accrediting Body (defined in Section IV(c), RDS User Accreditation) and attests that not only is their purpose Legal Action, but that data is being obtained to investigate possible trademark infringement by subject "X." User supplies name and contact information of the individual/organization that is the subject of interest. RDS Queries for this purpose are thus inherently limited to registration data associated with this subject.

Step 2) The RDS User may then perform a Reverse Query on values already known about the subject, searching the RDS for a list of domain names that include given values as:

- Registrant and/or PBC Name/Organization
- Registrant and/or PBC Phone/Alt Phone
- Registrant and/or PBC Postal addresses, or
- Registrant and/or PBC Email/Alt Email

Some of these data elements may be gated. The Reverse Query searches on these approved gated data elements, but only for the given value and stated purpose, as detailed in the attestation.

Step 3) Given a list of domain names under investigation for that might possibly be involved in the trademark infringement under investigation, the RDS User may now perform RDS Queries on those domain names to obtain data needed to evaluate cases, notably:

- Contact ID
- Registration Dates
- Registrar Jurisdiction
- Registry Jurisdiction
- Registrant Country (jurisdiction of the Registrant)
- Registrant Organization, and
- Registrant Company Identifier

This same information may also be requested in WhoWas queries for these domain names. In this step, all but one data element is public; the only gated data is the Registrant's country.

Step 4) Having concluded that further action is appropriate, the RDS User may perform an RDS Query to retrieve the published, public Legal Contact ID and associated contact data (including PBC Name/Organization, Phone, and postal address). These results may be used to attempt contact with the Registrant's designated Legal Contact, or may be used to file suit, bring a UDRP claim, or take some other legal action.

Step 5) If the Legal Contact denies responsibility for the domain name, the Registrant's full contact details may be necessary to take legal action. Much of this data may have been known in Step #1, not obtained from the RDS. However, some gaps may exist that need to be filled at this point.

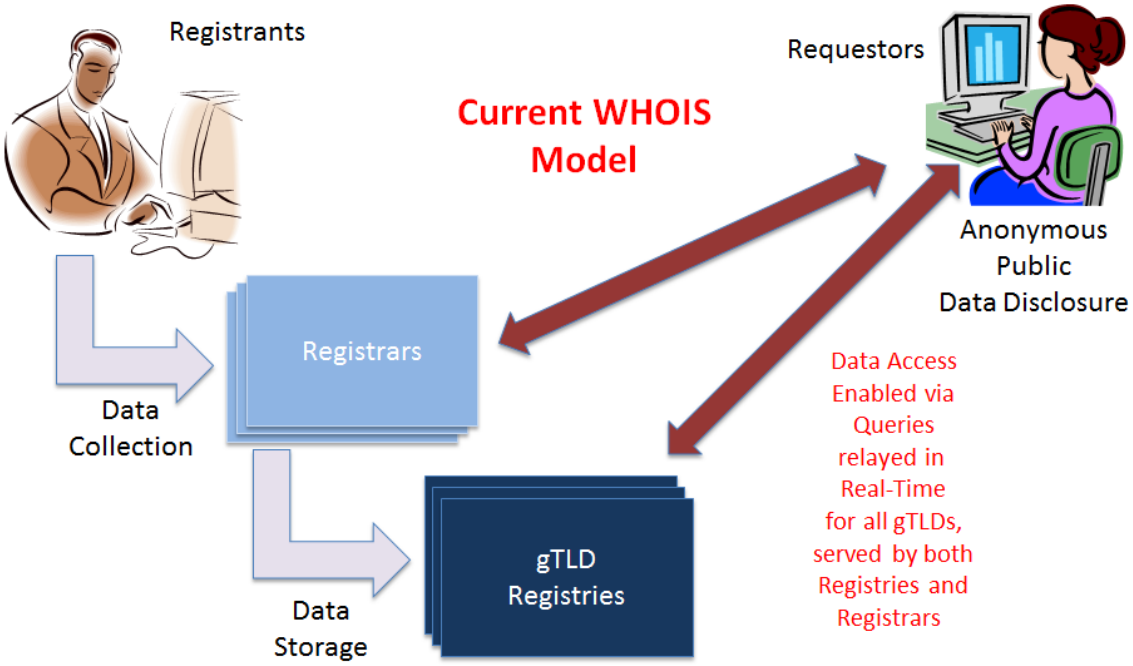
This example illustrates RDS interactions that might involve investigations and possible legal action pertaining to trademark infringement. However, a very similar series of steps may occur in other kinds of Legal Actions and when investigating domain name assets during a Purchase/Sale. In cases involving approved gated data, the Accreditor should be responsible for auditing access to detect requests that likely go beyond the asserted narrow scope and for taking steps to prevent abuse and enforce ToCs. Having the attestation of the RDS User on file will help the Accreditor audit access and investigate possible abuse. It will also serve as a deterrent to fishing expeditions.

ANNEX F: SYSTEM MODELS CONSIDERED AND METHODOLOGY

In addition to the models previously described in Possible RDS Models, the EWG considered the following alternatives but found each less viable than the Federated or Synchronized Models, for reasons summarized below.

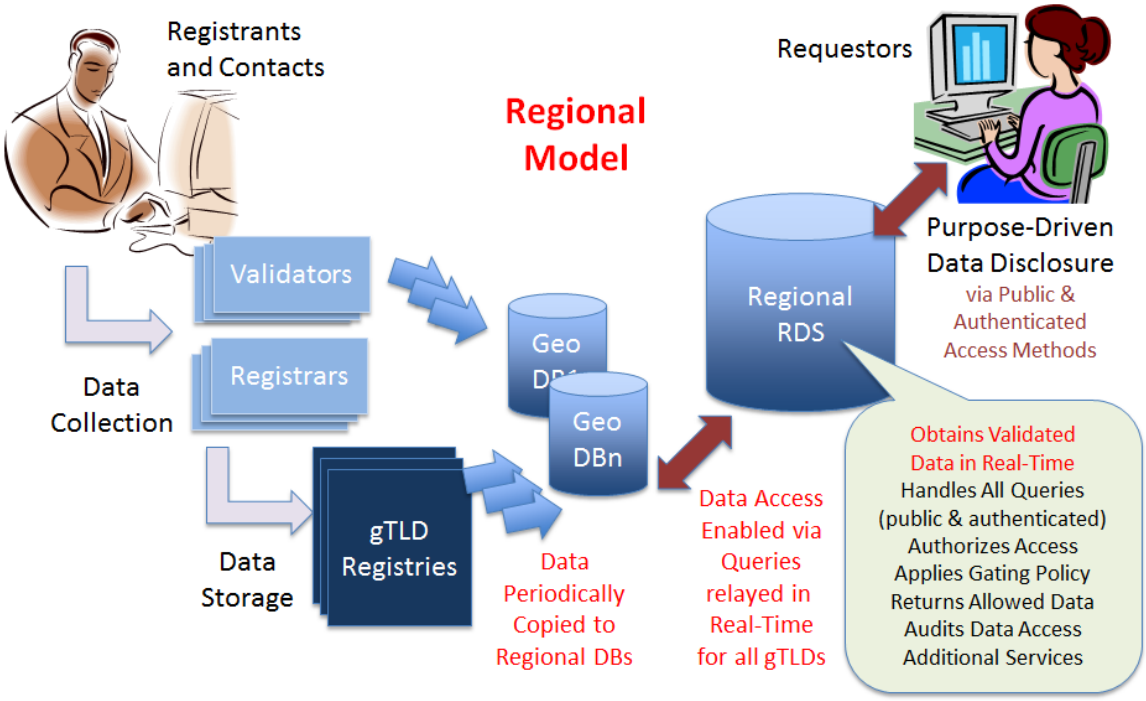
Current WHOIS

This model describes the fully-distributed autonomous approach employed by today's WHOIS system, with each Registry and Registrar offering its own WHOIS services without integration across all gTLDs. Although a centralized portal to enable access to WHOIS across all gTLDs could be built, each Registry would still provide its own independently-managed storage and access, either directly (thick) or via delegation to Registrars (thin).



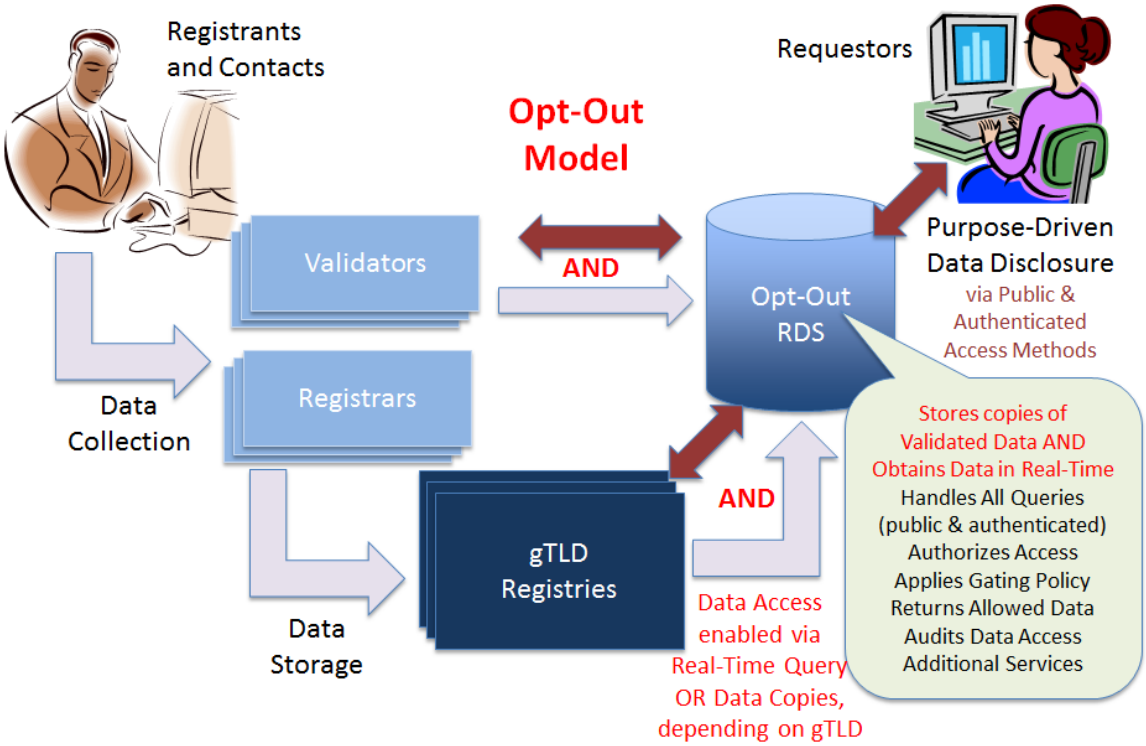
Regional Model

This model describes an RDS that periodically copies data from distributed storage areas operated by Registries and Validators into regional storage areas located around the world. Registries and Validators continue to store data, but regional copies of that data can be used by the RDS to process access requests more effectively. Regional storage areas are operated by the RDS but are subject to laws of the jurisdiction in which each is located.



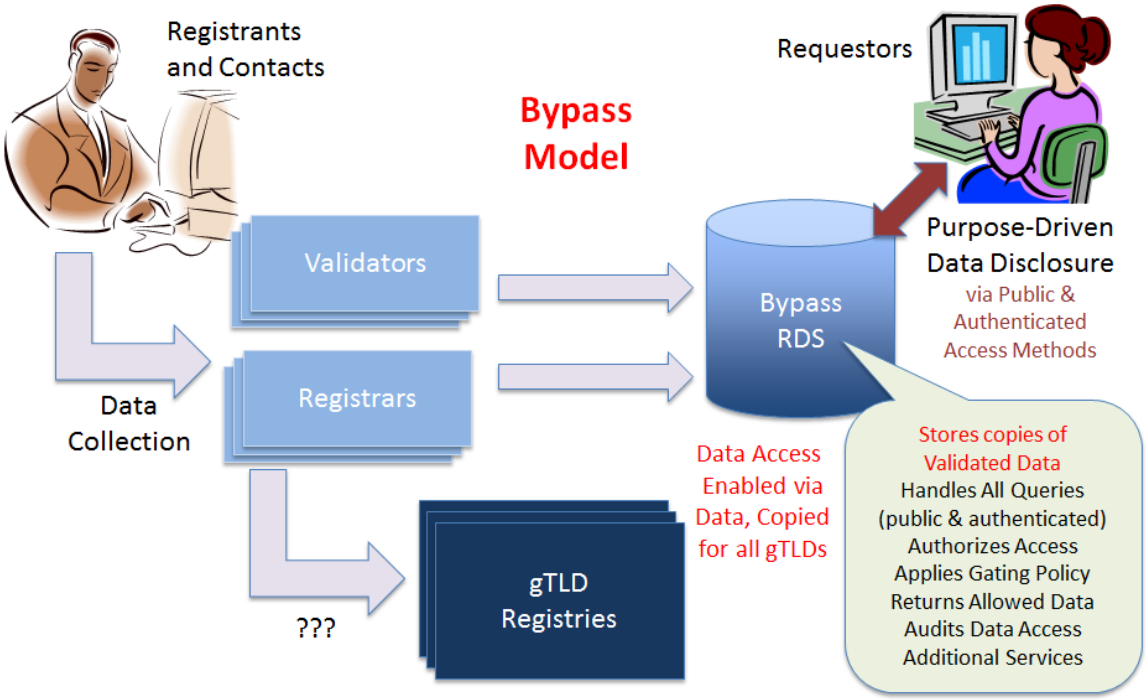
Opt-Out Model

This model describes an RDS that periodically copies data from distributed storage areas operated by Registries into a synchronized storage operated by the RDS. Under this model, any Registry can opt out of synchronized storage so long as they agree to provide the necessary infrastructure to handle significant querying required under availability and performance service level agreements (SLAs).



Bypass Model

This model describes an RDS that periodically copies data from distributed storage areas operated by Registrars into synchronized storage operated by the RDS. Under this model, Registries are bypassed as a source of registration information; instead, the RDS services queries using synchronized registration data copied directly from authoritative sources.



Methodology Applied to Compare System Models

The EWG considered the attendant costs and security vulnerabilities inherent in the current WHOIS system, many of which are addressed in the reports listed in Annex B that document deficiencies in WHOIS. The costs and vulnerabilities of the current WHOIS system were compared and contrasted with the possible models. In addition, the EWG compared the security pros and cons of each of the possible models against the following criteria:

Security Implications

- **Single Point of Failure:** Taking into account the use of distributed architecture and a primary service provider, how vulnerable is the model to any single system failing? Would failure of any system temporarily prevent access to all or only some registration information? **Note:** Sound database design and operating practices should be used to provide internal redundancy and data backup, so this is really about data availability during failure.
- **Subject to Internal Abuse:** How vulnerable is the model to insider-abuse of administrative/operator access to registration information stored by or passing through any system that makes up the model? Would insider-abuse result in unauthorized access to all or some data? How easily could controls be applied to detect/deter insider-abuse?
- **Subject to External Attack:** How vulnerable is the model to external attack against any system that makes up the model? Would an outside attack result in privacy breach for all or some Registrants? How easily could controls be applied to detect/deter external attack?
- **Security Consistency:** How vulnerable is the model to inconsistent security implementation and policy enforcement? Are security goals likely to be met uniformly by all of the players responsible for operating components of the system? Or would security be heavily impacted by differences in Registrar/Registry/Validator expertise and investment?

Jurisdiction and Privacy Implications

- **Stores data in local jurisdictions:** Does the model allow for storage of registration information in one of several jurisdictions? To what extent could Registrants or Registrars/Validators choose to store registration information in a jurisdiction with data protection laws that are compatible with the Registrant's local jurisdiction?

- **Enables application of local laws to display:** Does the model allow for access of registration information in a manner compatible with one of several jurisdictions? To what extent could the RDS apply the data protection laws of the Registrant's local jurisdiction to registration information that is accessed through the RDS?
- **Enables compliance with local data protection laws:** Does the model help or hinder Registrar and Registry compliance with the local data protection laws that apply to them? How cumbersome would the model make it to obtain exceptions needed to enable compliance? How will adherence to the legal procedures required by the local law of the Registrant be ensured?

Accreditation

- **Enables Requestor Accreditation:** Does the model let users wanting purpose-drive access to gated data apply for accreditation, be vetted, receive access credentials, and use them to gain appropriately authorized access to data? To what extent does the model help or hinder uniform, robust application of such a requestor accreditation process?

  Validation: Does it make it easier? Does it make it less costly? Does any system make Secure Credentials easier or cheaper?
- **Track/Penalize Requestors:** How effectively and reliably can the model log data access requests and responses for the purposes of detecting abuse of accredited access (i.e., actions that violate terms and conditions of access)? To what extent does the model help or hinder compliance enforcement actions (e.g., penalties applied to non-compliant users to deter future abuse)?
- **Audit:** Does the model enable auditing of data access requests and responses and related operations, to assess the efficacy of the accreditation process and authorized access to data?

Operation

- **User-friendly portal:** Does the model allow user-friendly presentation of registration information displayed through a web portal or returned in response to protocol queries? To what extent does the model support internationalization principles (e.g., support for local character sets, response translation)? To what extent does the model facilitate consistent display across all gTLDs?

- **Random Data Audits/Accuracy Reports:** Does the model support periodic accuracy audits and accuracy reporting across all gTLDs? To what extent does the model facilitate efficient, consistent detection and updating of inaccurate registration information and uniform enforcement of accuracy policies?
- **Data Latency (Performance):** Does the model have inherent inefficiencies in data handling that are likely to degrade performance and cannot be addressed through scalable platform implementation? What is the relative magnitude of those inefficiencies (as compared to other models) for the speed of handling requests and delays perceived by users that query registration information?
- **Data Synchronization:** Does the model require data copied from any system to be synchronized with other systems? How extensive are these data synchronization needs and how problematic will any temporary lack of synchronization be (as compared to other models)?
- **Registrant access to own data:** Does the model support or prevent Registrant access to his/her own registration data?
- **Storage/escrow requirements:** Does the model introduce multiple storage areas that increase the number or complexity of data storage and escrow requirements?
- **Enables Pre-validation Measures:** Does the model support pre-validation of Registrant and Purposed-Based Contact information across all gTLDs? To what extent does the model facilitate efficient, consistent creation and maintenance of pre-validated contact information and uniform enforcement of any related uniqueness policies?

Implementation

- **Complex infrastructure:** Is the model less complex overall, as compared to other models? For example, a more complex (weaker) model might have many more systems and interfaces that will require initial investment and on-going maintenance.
- **Ease of Implementation:** Is the model likely to be easier to implement, as compared to other models? For example, a more difficult (weaker) model might require changes to more systems.
- **Ease of Transition:** How well does the model facilitate a smooth transition from today's WHOIS to a next-generation RDS, as compared to other models? Here, a weaker model is one that makes it harder for users, Registrars, and Registries to transition from existing processes.

Cost

- **Reduces Registrar and Registry WHOIS Operating Costs:** Will the model be likely to reduce on-going operating and maintenance cost to Registrars and Registries, as compared to the current WHOIS system? Here, a model that reduces cost is considered stronger.
- **Lower Cost of Implementation:** Will the model require more or less initial investment overall in new/modified infrastructure and processes, as compared to other models? Here, a model with lower overall cost of implementation is considered stronger.
- **Reverse Query & Historical WhoWas:** Will the model require additional investment to accommodate Reverse Query and historical WhoWas searches by authorized requestors? In this instance, a model requiring a lower total cost to deliver these services is considered stronger.

Use Cases

Comparing the ability of these possible models to support all users and purposes identified in the Initial Report, including (but not limited to) the following gTLD use cases:

- Domain Name Acquisition
- Domain Name Registration History (including tracking the registration history of any domain name (WhoWas))
- Domain Names for Specified Registrant (including finding every domain name registered by a specific Registrant (Reverse RDS query))
- UDRP Proceedings
- Investigate Abusive Domain Name
- Deter Malicious Internet Activities

Model Cost Analysis

To examine implementation feasibility and costs associated with the SRDS and FRDS models, ICANN engaged IBM to develop a detailed analysis focused on cost differences between these two possible implementation models. IBM produced a final report entitled "*Registration Directory Service (RDS) Implementation Model Cost Analysis*[40]." An excerpt of IBM's findings, taken from their report, is reproduced here for reference.

[40] https://community.icann.org/display/WG/EWG+Public+Research+Page

Approach

During February/March 2014 a budgetary cost analysis was conducted, comparing the realization of Synchronized[41] and Federated RDS implementations. A phased approach was used:

- *Step 1: Gather baseline requirements for each of the implementation models.*
- *Step 2: Define and agree key volumetric assumptions provided by ICANN and based largely upon monthly WHOIS query reports supplied by gTLD Registries. Use these assumptions to derive the expected system workload and define a high level baseline solution outline for each of the two implementation models.*
- *Step 3: Create cost model and perform a budgetary costing of each of the baseline solution outlines.*
- *Step 4: Formulate findings.*

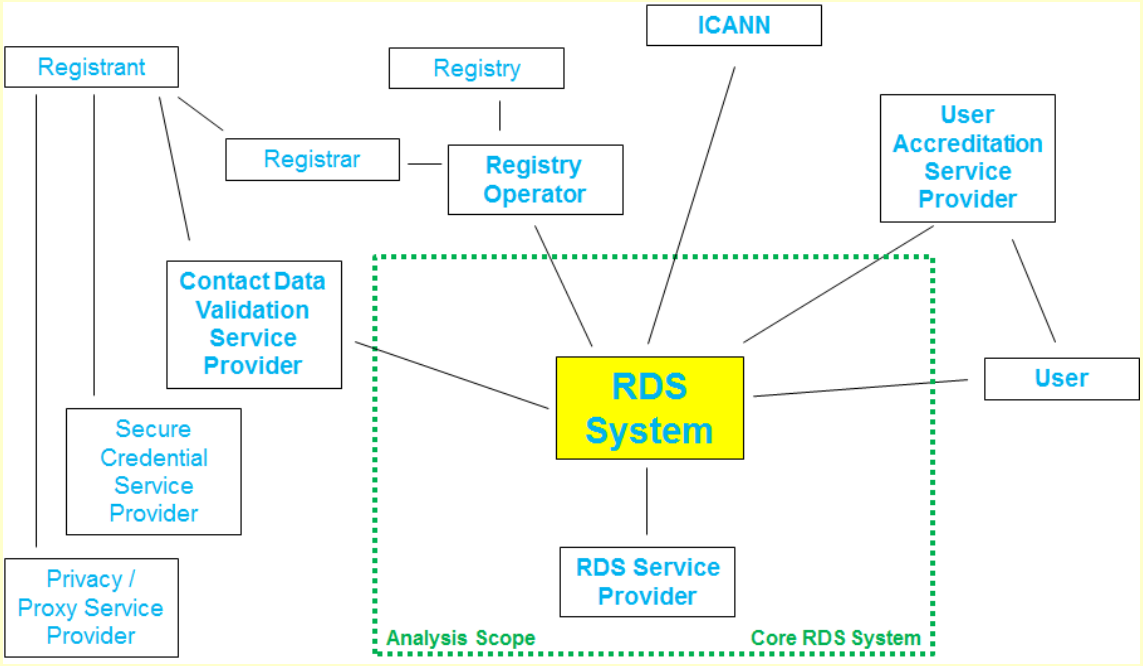
Engagement Starting Points

- *Create a budgetary cost estimate for the central "RDS system/provider". Registry Operator costs are not estimated.*
- *A Managed Service cost model and estimate is created. That is, assume the setup and ongoing operations of a managed RDS service and estimate the related costs.*
- *For purposes of cost comparison, the solution and costs are based largely on IBM's portfolio (primarily IBM's SoftLayer IaasS offering), using third party solution components only where no alternative exists in the IBM portfolio.*
- *Cost estimations are created for the baseline requirement/solution outline only, not for variants; no detailed cost driver analysis is performed.*

[41] For alignment with the EWG's Final Report, this summary refers to the Synchronized RDS (SRDS), the model described in earlier EWG reports as the Aggregated RDS (ARDS).

Core Analysis Scope and Volumetrics

The focus of the cost analysis was the "Core RDS System" as depicted below



.

The core use cases to support in each of the models (Synchronized and Federated) were defined.

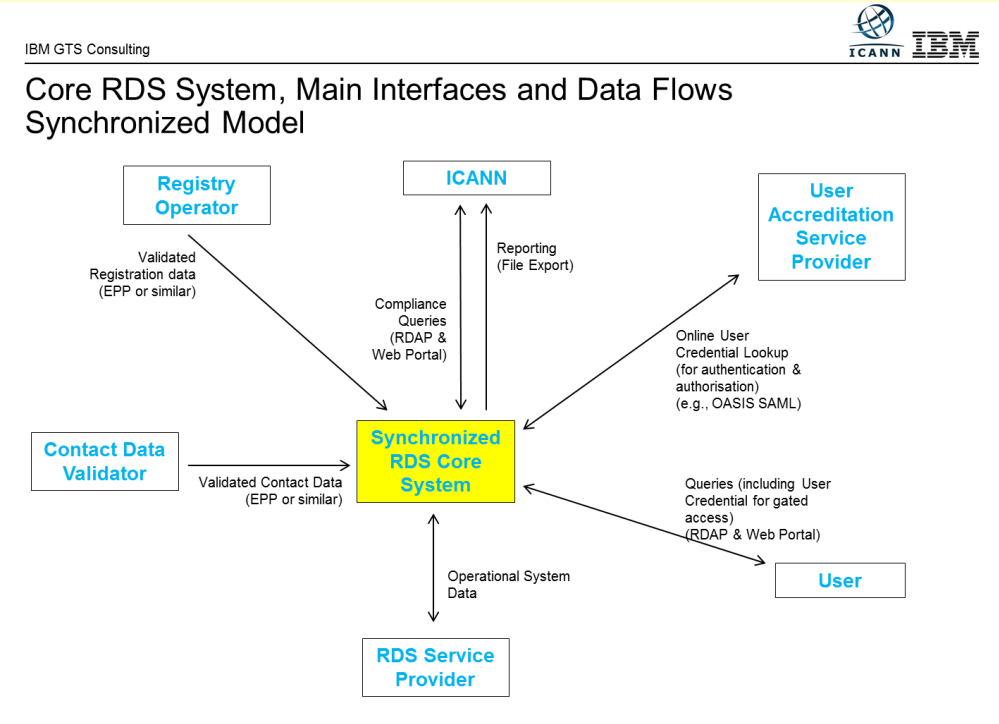
In addition, key volumetric assumptions were defined:

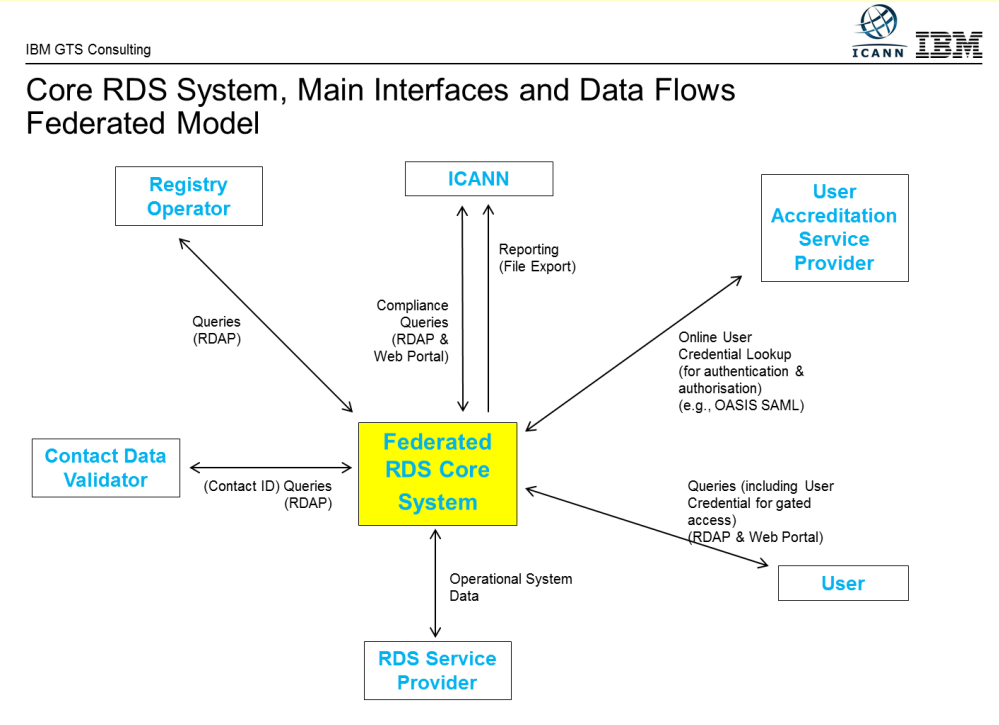
YEARLY GROWTH RATE	22%	nr of DN records added in a year, assumed to include the growth in the nr of gTLDs					
Nr of DN RECORDS, YEARLY UPDATE RATE	100%	nr of DN records updated in a year					
		start yr1 (2015)	start yr2 (2016)	start yr3 (2017)	start yr4 (2018)	start yr5 (2019)	end yr 5 (2020)
Nr of gTLDs		2000	3000	4000	5000	6000	7000
growth rate			50%	33%	25%	20%	17%
	December 2013, ICANN input	start yr1 (2015)	start yr2 (2016)	start yr3 (2017)	start yr4 (2018)	start yr5 (2019)	end yr 5 (2020)
NR OF DOMAIN NAMES	151.196.101	184.459.243	225.040.277	274.549.138	334.949.948	408.638.936	498.539.502
NR OF QUERIES/MONTH	9.031.522.529	11.018.457.485	13.442.518.132	16.399.872.121	20.007.843.988	24.409.569.665	29.779.674.992
AVERAGE NR OF QUERIES/SEC	3.484	4.251	5.186	6.327	7.719	9.417	11.489
NR OF QUERIES/PEAK SEC		42.509	51.862	63.271	77.191	94.173	114.891
AVERAGE NR OF QUERIES/HOUR	12.543.781	15.303.413	18.670.164	22.777.600	27.788.672	33.902.180	41.360.660
NR OF QUERIES IN PEAK HOUR	25.087.563	30.606.826	37.340.328	45.555.200	55.577.344	67.804.360	82.721.319
USER VISITS IN PEAK HOUR	16.892.292	20.608.596	25.142.488	30.673.835	37.422.079	45.654.936	55.699.022
CONCURRENT VISITS IN PEAK HOUR	563.076	686.953	838.083	1.022.461	1.247.403	1.521.831	1.856.634
NEW VISITS IN PEAK SEC		28.623	34.920	42.603	51.975	63.410	77.360

% of reverse queries	1,0%

RDS Implementation Models

The following implementation models were derived from the EWG's Initial and Status Update Reports for purposes of cost analysis:



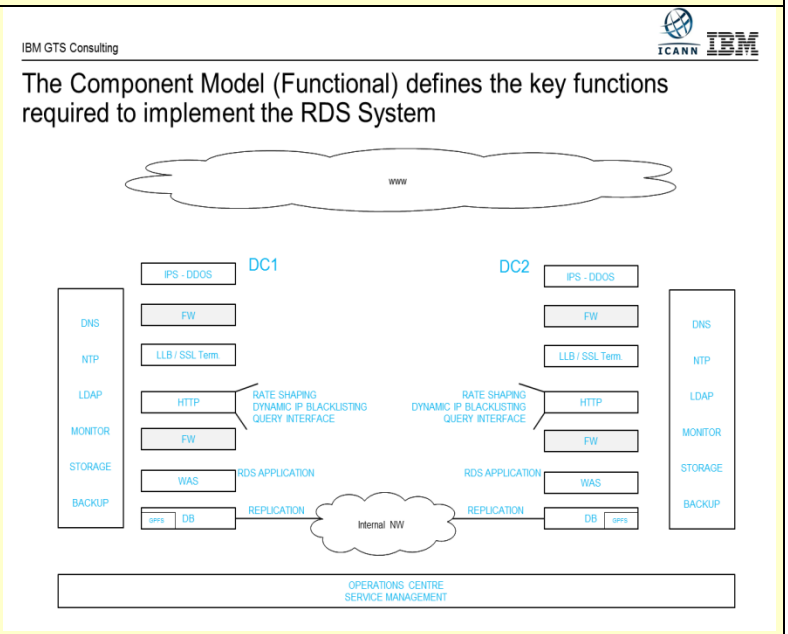


RDS Functional Components

The following component model was created for purposes of cost analysis, incorporating all of the key functions required to implement the RDS system. Standard systems design best practice assumptions were used when costing both the SRDS and FRDS, such as replicating the RDS core system and database across two geographically diverse data centers, with load balancing and fail-over to ensure redundancy and availability, and IPS to deflect DDoS. It should be understood that these functional components APPLY TO BOTH IMPLEMENTATION MODELS.

Functional Components:

- *Inter-DC Load Balancing/Routing*
- *IPS DDoS Mitigation*
- *Intra-DC Load Balancing & SSL*
- *Web (HTTP) Server*
- *Web Application Server (WAS)*
- *WAS Admin Node*
- *Database (DB) Caching System*
- *DB Member System*
- *Storage Server*
- *Systems Monitoring*
- *DNS*
- *NTP*
- *LDSP*
- *Syslog Repository*
- *Backup Server*
- *Backup Storage Server*
- *DB Backup Client System*
- *Network Zoning, Firewall/IPS*
- *Internet and DC Connectivity*



For example, a two Data Center setup was assumed for the core RDS system in both the SRDS and FRDS model, using an active-active design where each core RDS is capable of handling 50% of peak load. This cost analysis did not include clustering for High Availability within each data center; this could be added without changing the relative costs of the two RDS models.

Cost Estimates (assuming 1% Reverse queries)

The costing summarized below does in no sense constitute an IBM implementation proposal. The costing has been created for the sole purpose of and is only to be used and considered as part of a budgetary costing analysis aimed at comparing two RDS implementation models. Based on the key volumetric inputs, workload requirements, and solution outline given above, the cost per domain name per year for the ***Core FRDS and SRDS Systems only*** *are estimated as:*

SRDS Budgetary Cost Estimate

€ 0,0183 average cost/domain/year

cost per domain name

yr1	yr2	yr3	yr4	yr5
€ 0,041	€ 0,023	€ 0,017	€ 0,020	€ 0,019

FRDS Budgetary Cost Estimate

€ 0,0173 average cost/domain/year

cost per domain name

yr1	yr2	yr3	yr4	yr5
€ 0,041	€ 0,018	€ 0,017	€ 0,021	€ 0,017

Differences in cost were further analyzed and compared as follows:

FRDS – SRDS Budgetary Cost Estimate Differences

SETUP COSTS		**5,9%**		10,5%	
INFRASTRUCTURE SETUP COSTS	ARCHITECTURE & DESIGN	**1,5%**	0,2%	15,6%	0,0%
	PROVISION & CONFIGURE		1,2%		19,2%
	INFRASTRUCTURE TESTING		0,1%		18,4%
APPLICATION SETUP COSTS	ANALYSIS, DESIGN, CODE, UNIT TEST	**1,2%**	1,2%	0,0%	0,0%
TESTING	INTEGRATION TESTING & DEPLOYMENT	**1,7%**	0,8%	7,8%	0,0%
	E2E SYSTEM TESTING		0,2%		38,2%
	PERFORMANCE		0,2%		33,3%
	SECURITY (ETHICAL HACK)		0,5%		0,0%
TRANSITION TO BAU	TRANSITION TO BAU	**0,6%**	0,5%	26,6%	37,7%
	SERVICE DESK SETUP		0,1%		0,0%
MANAGEMENT	PROJECT MANAGEMENT	**0,9%**	0,9%	13,4%	13,4%

The FRDS model implies a higher computing power requirement (more systems required to handle the envisaged load) in the web and web application server layer.

Due to a higher amount of systems to interface with in an on-line manner when handling queries, the FRDS model is estimated to involve more testing effort

FRDS – SRDS Budgetary Cost Estimate Differences

COST MODEL FRDS		SHARE IN TOTAL		DIFFERENCE WITH ARDS	
		100,0%		-5,4%	
RUN COSTS		94,1%		-6,3%	
INFRASTRUCTURE COSTS	PUBLIC NW	**30,5%**	8,1%	-22,4%	-55,9%
	DC NW, GLB, LLB, IPS/DDOS		5,7%		10,7%
	HTTP SERVERS		2,2%		236,0%
	WAS SERVERS		3,7%		218,5%
	DB SERVERS		2,2%		-52,0%
	STORAGE		6,3%		-3,8%
	BACKUP		1,9%		-19,0%
	GENERIC SYSTEMS		0,3%		0,0%
SW LICENCE & MAINTENANCE COSTS	DB	**32,7%**	13,7%	-17,5%	-59,5%
	WAS		18,8%		234,6%
	BACKUP		0,3%		0,0%
OPERATIONS AND MANAGEMENT COSTS	INFRA OPERATIONS & MAINTENANCE	**30,9%**	19,4%	44,0%	63,6%
	APPLICATION OPERATIONS		2,6%		20,0%
	APPLICATION MAINTENANCE		1,3%		27,3%
	SERVICE GOVERNANCE		5,2%		0,0%
	SERVICE DESK		2,4%		100,0%

The Public NW cost is lower in the FRDS case due to the IBM SoftLayer NW charging model: incoming traffic is free; per server 20 TB/month outgoing traffic is free, i.e. you get a total free outgoing volume of #servers x 20 TB per month. As the number of servers increases in the FRDS model, the total amount of free TB outgoing NW volume/month increases.

The FDRS model implies a higher NW throughput requirement. Impact on Firewall and Intrusion Prevention Component.

The FRDS model implies a higher computing power requirement in the web and web application server layer.

The FRDS model implies less storage and backup storage capacity as less data is stored centrally.

The DB compute requirement is estimated to be higher in the SRDS model.

Due to a higher amount of systems to interface with in an on-line manner when handling queries, the FRDS model is estimated to involve a higher application operations, support & maintenance release testing workload

Main Conclusions

With the assumptions used, the Core RDS system is slightly less expensive in the Federated RDS (FRDS) model than the Synchronized RDS (SRDS) model.

The FRDS model is highly sensitive to variations in the Reverse Query load. With a higher amount of Reverse Queries, the FRDS model becomes substantially more expensive: With a 3% Reverse Query load instead of a 1% Reverse Query load, the cost of the FRDS model is estimated to increase close to 35%. This is an important factor of uncertainty and risk associated with the FRDS model. The SRDS model to the contrary is believed to be less sensitive to the amount of Reverse Queries.

The FDRS model is expected to require higher application operations, support, maintenance, and test effort as more interactions with Registry Operators are expected.

In addition, the FRDS model has more impact on the Registry Operators. In the FRDS model, each Registry Operator will have to implement support - under SLA - for online queries, including Reverse Queries and historical ownership queries (aka WhoWas). For the latter historical data would have to be maintained by the Registry Operators.

ANNEX G: ABILITY OF EPP AND RDAP PROTOCOLS TO SUPPORT RDS

Data Element	EPP Support for Collection	RDAP Support for Access
Domain Name	Y	Y
Registration Status	Y	Y
DNS Servers	Y	Y
DNSSEC Delegation	Y	Y
Client Status	Y	Y
Server Status	Y	Y
Registrar	Y	Y
Reseller	Y	Y
Registrar Jurisdiction	N	N
Registry Jurisdiction	N	N
Registration Agreement Language	N	Y
Creation Date	Y	Y
Original Registration Date	Y	Y
Registrar Expiration Date	Y	Y
Registrant Type	N	Y*
PBC Name	Y	Y
PBC ID	Y	Y
PBC Validation Status	N	N
PBC Last Validated Timestamp	N	N
PBC Organization	Y	Y
PBC Street Address	Y	Y
PBC City	Y	Y
PBC State/Province	Y	Y
PBC Postal Code	Y	Y
PBC Country	Y	Y
PBC Email Address	Y	Y

Data Element	EPP Support for Collection	RDAP Support for Access
PBC Alt Email Address	N	Y
PBC Phone + Ext	Y	Y
PBC Alt Phone + Ext	N	Y
PBC Fax + Ext	Y	Y
PBC SMS	N	Y
PBC IM	N	Y
PBC Social Media, Alt SM	N	Y
PBC Contact & Abuse_URLs	N	Y
Updated Date	Y	Y
Registrant Name	Y	Y
Registrant Contact ID	Y	Y
Registrant Contact Validation Status	N	N
Registrant Contact Last Validated Timestamp	N	N
Registrant Organization	Y	Y
Registrant Company Identifier	Y	Y
Registrant Street Address	Y	Y
Registrant City	Y	Y
Registrant State/Province	Y	Y
Registrant Postal Code	Y	Y
Registrant Country	Y	Y
Registrant Phone + Ext	Y	Y
Registrant Fax + Ext	Y	Y
Registrant Email, Alt Email Address	Y	Y
Registrant SMS	N	Y
Registrant IM	N	Y
Registrant Social Media, Alt SM	N	Y
Registrant Contact & Abuse_URLs	N	Y
Registrar URL	N	Y

Data Element	EPP Support for Collection	RDAP Support for Access
Registrar IANA Number	N	Y*
Registrar Abuse Contact Email Address	N	Y
Registrar Abuse Contact Phone Number	N	Y
URL of Internic Complaint Site	N	Y

*These data elements are not explicitly specified in RDAP. They can be returned using "remarks" fields or a protocol extension.

Protocol Extensions and/or Additions

Registrar and Registry Jurisdiction: Would need to be added to EPP or derived from current Registrar location information. Can be returned using RDAP entity "remarks" or via a protocol extension.

Registration agreement language: Would need to be added to EPP by protocol extension.

Registrant type: Would need to be added to EPP by protocol extension.

Registrant/PBC Validation Status, Last Validated Timestamp, Alt Email, Alt Phone + Ext, SMS, IM, Social Media, Alt Social Media, Contact_URL, Abuse_URL: Would need to be added to EPP by protocol extension. RDAP can handle social media identifiers, but a specification would need to be created to define the format for such identifiers.

Type of Contact: The currently available types are "admin," "billing," and "tech." Additional contact types would require an extension to RDAP

Stated purpose in RDAP Query: Would need to be added to RDAP by protocol extension.

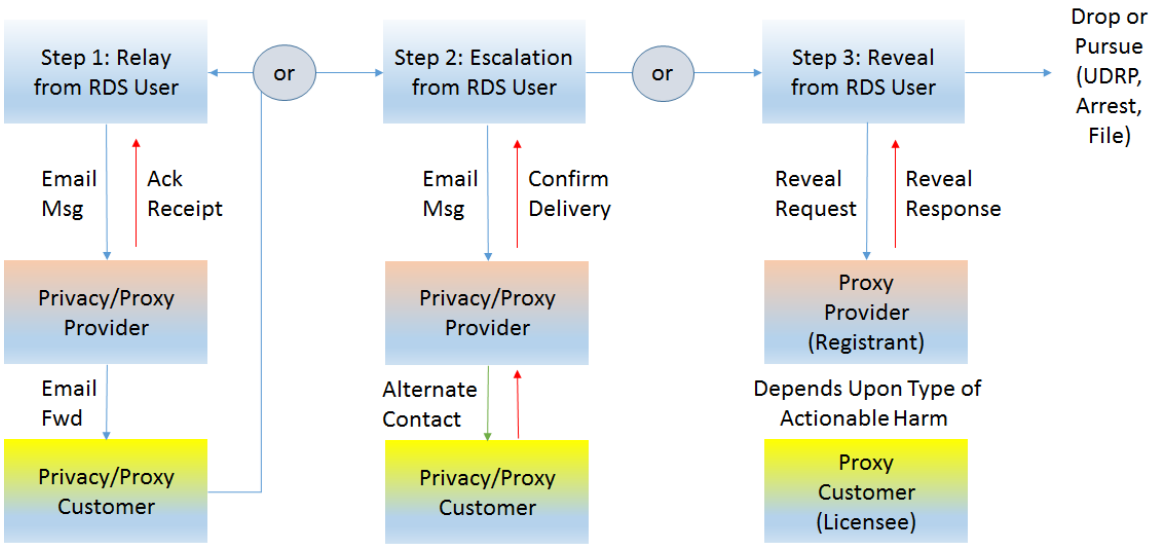
Access Level in EPP: EPP includes a simple mechanism to collect and pass Registrant contact element disclosure preferences from Registrar to Registry, where they can be used to inform RDAP response behavior. However, this mechanism is not granular enough to capture preferences at the level of each individual data element. A new EPP extension and/or contact mapping would therefore be needed to indicate the Registrant's or contact's choice to override disclosure defaults for each data element (e.g., choosing to publish an element that is gated by default).

ANNEX H: MODEL AND PRINCIPLES FOR RELAY AND REVEAL

As noted in Section VI(b), the EWG recommends accredited Privacy and Proxy Services be required to relay all email received by the forwarding email address. The goal is to provide accredited Privacy/Proxy customers and RDS users who might want to contact them with a standard, always-available, near real-time communication path.

In addition, the EWG recommends requiring accredited proxy services respond to reveal requests in a timely manner (further details below). The goal is to provide users experiencing serious problems with proxy-registered domains with a standard, always-available, efficient process to seek effective problem resolution.

When analyzing these user needs, the EWG noted another shortfall in today's practices: the absence of a readily-available, efficient escalation method when communication fails. Many users jump quickly to reveal because they have no other recourse. The EWG recommends introducing an escalation process which might be less costly to all parties and reduce the number of problems that lead to more costly and time-consuming reveal requests. This three-step process is illustrated below:



Step 1: Relay

a) The RDS user requests contact data for a domain, retrieving:

- The Registrant's Contact ID (i.e., the Privacy Customer or Proxy Provider's Contact ID)

- Contact IDs for all mandatory Purpose-Based Contacts (PBCs) and published PBC addresses (including email addresses)

- An indication the domain registration was done via Privacy/Proxy Service, and

- Name and address of the accredited Privacy or Proxy Service Provider, provided as a Privacy/Proxy Provider PBC, which includes a published Relay Escalation and Reveal form URLs.

b) The RDS user, noting that this is an accredited Privacy/Proxy registration, attempts to email the Privacy/Proxy customer at the forwarding address. Providers might optionally let customers supply more forwarding addresses (e.g., phone, SMS, postal).

c) The accredited Privacy/Proxy provider must be required to forward and acknowledge receipt of the relayed message (e.g., email acknowledgement to all messages received for the forwarding email address). A negative acknowledgement might be returned for error cases (e.g., no such mailbox), and acknowledgements to the same sender might be limited by a threshold to deter relay abuse.

d) The RDS user receiving the acknowledgement now has confirmation that the message was relayed to the Privacy/Proxy customer. However, the customer may choose not to reply or may discard the relayed message without reading it (e.g., treat as spam).

Step 2: Escalation

The RDS user tires of waiting for the accredited Privacy/Proxy customer to respond and decides to escalate the previously-attempted contact by:

a) Visiting the website of the accredited Privacy or Proxy Service identified in Step 1 and completing an escalation form that contains:

- The RDS user's identity (possibly re-using an RDS query credential)

- The RDS user's reason for contact (could be a pull-down list of defined reasons)

- The Privacy/Proxy-registered domain name

- An uploaded message to be relayed to the customer (possibly encrypted?)

- Timestamp of when relay was first attempted

b) The accredited Privacy/Proxy Provider must be required to try to contact the customer directly, possibly using contact information and/or methods inaccessible to

the RDS user, returning a "delivery confirmation" within N*[42] days. Here again, negative confirms would be returned for error cases (e.g., unauthenticated user, timeout) and submissions could be logged and limited by a threshold to deter abuse.

c) The RDS user receiving the confirmation now has documented proof that the message was delivered to the Privacy/Proxy customer. The customer may still choose not to reply, but escalation must help overcome basic communication failures without requiring reveals.

Step 3: Reveal (only applies to proxy-registered domains)

The RDS user times out waiting for the accredited Proxy customer (licensee) to respond and decides the problem is significant enough to pursue criminal or civil action by:

a) Visiting the website or calling or mailing the accredited Proxy Service Provider identified in Step 1 and submitting a reveal request that contains:

- The RDS user's identity
- The RDS user's reason for contact (narrowly limited to actionable harms)
- The Proxy Provider-registered domain name
- Documentation of harm (trademark registration information, allegations of abuse)
- Timestamp of when relay/escalation was attempted (case number from escalation?)

b) The accredited Proxy Provider must be required to investigate and take appropriate action (see d), returning a "reveal response" within N*[43] days. Reveal requests could be logged and limited to actionable harms alleged by RDS users with standing,[44] to deter abuse.

---

[42] * The timeout might depend on authenticated identity and stated reason for contact. For example, 1 day for law enforcement/OpSec investigating a crime/abuse; 7 days for brand owners investigating TM infringement; 7 days for Internet consumers trying to reach online merchants.

[43] * The timeout might depend on requestor and stated reason for contact. Law enforcement might go directly to Step 3 (Reveal) for time-sensitive investigations. Time frames and efforts for Step 2 must be low enough to discourage others from jumping directly to Step 3.

[44] ** Any user requesting a reveal must demonstrate they are (or represent) a party suffering actionable harm. For example, brand holders or their agents alleging TM infringement might show they own domain name(s) similar to the proxy-registered domain. Further thought is needed to map types of users to types of harms. See GoDaddy's list of proxy-registered domain complaint form options as example.

c) The accredited Proxy Provider, given documentation with which to assess the case, might:

- Notify and transfer the domain to the customer (that is, discontinue proxy service)
- Temporarily suspend the domain during a criminal investigation
- Reveal to the user the identity/contact of a licensee engaged in unlawful activity
- Reject the reveal – positively affirming the Proxy's liability for further domain use.

A policy must be developed here to detail what constitutes sufficient documentation and when the licensee must be notified. In addition, there will need to be clear policies regarding the impact of local law and factors to be considered. All of the above happens today, without any oversight, policy guidance or consequences for rejecting/ignoring reveal.

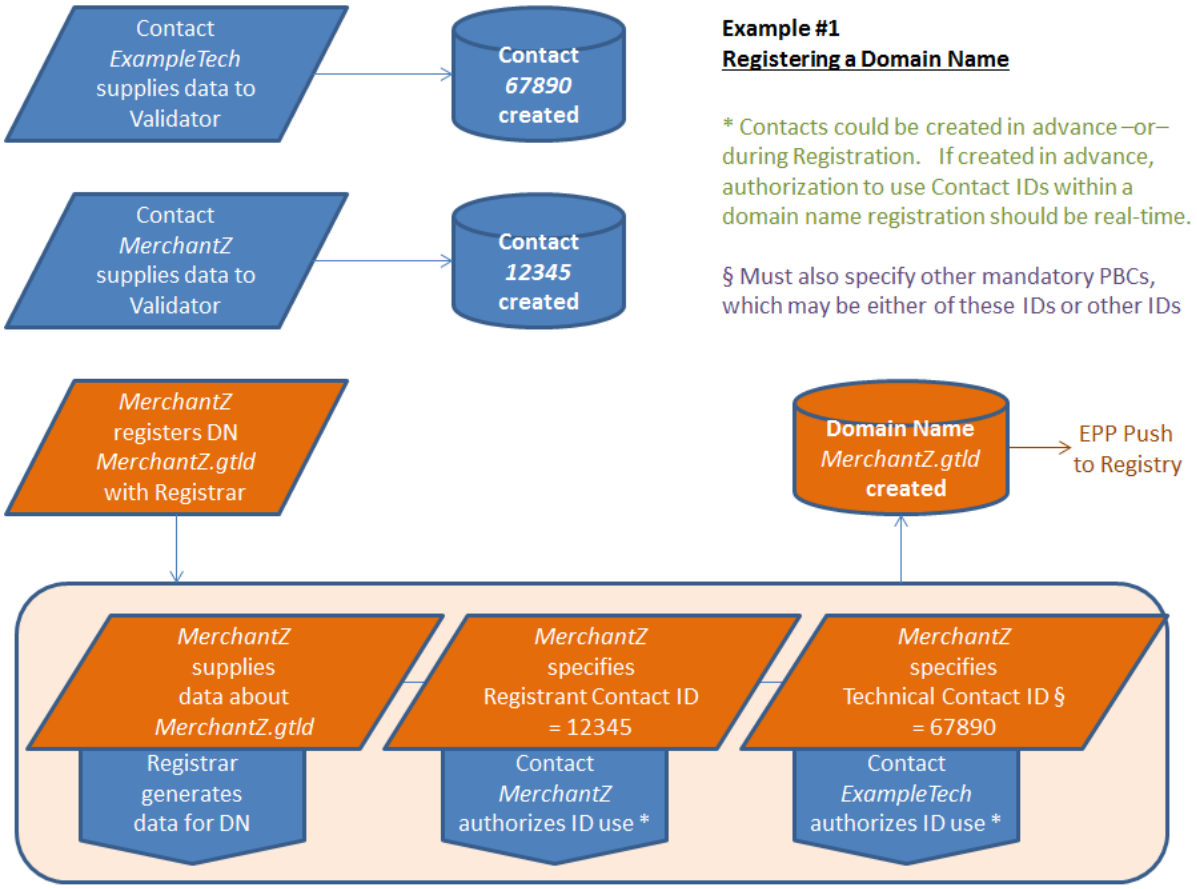
d) The RDS user receiving the reveal response now has the information needed to drop the matter or pursue legal/civil action. For example, trademark infringement might lead to filing a UDRP, while a law enforcement criminal investigation might lead to a suspect's apprehension. If the reveal is rejected (or timely response is not received), the RDS user may also now choose to pursue legal/civil action against the accredited Proxy.

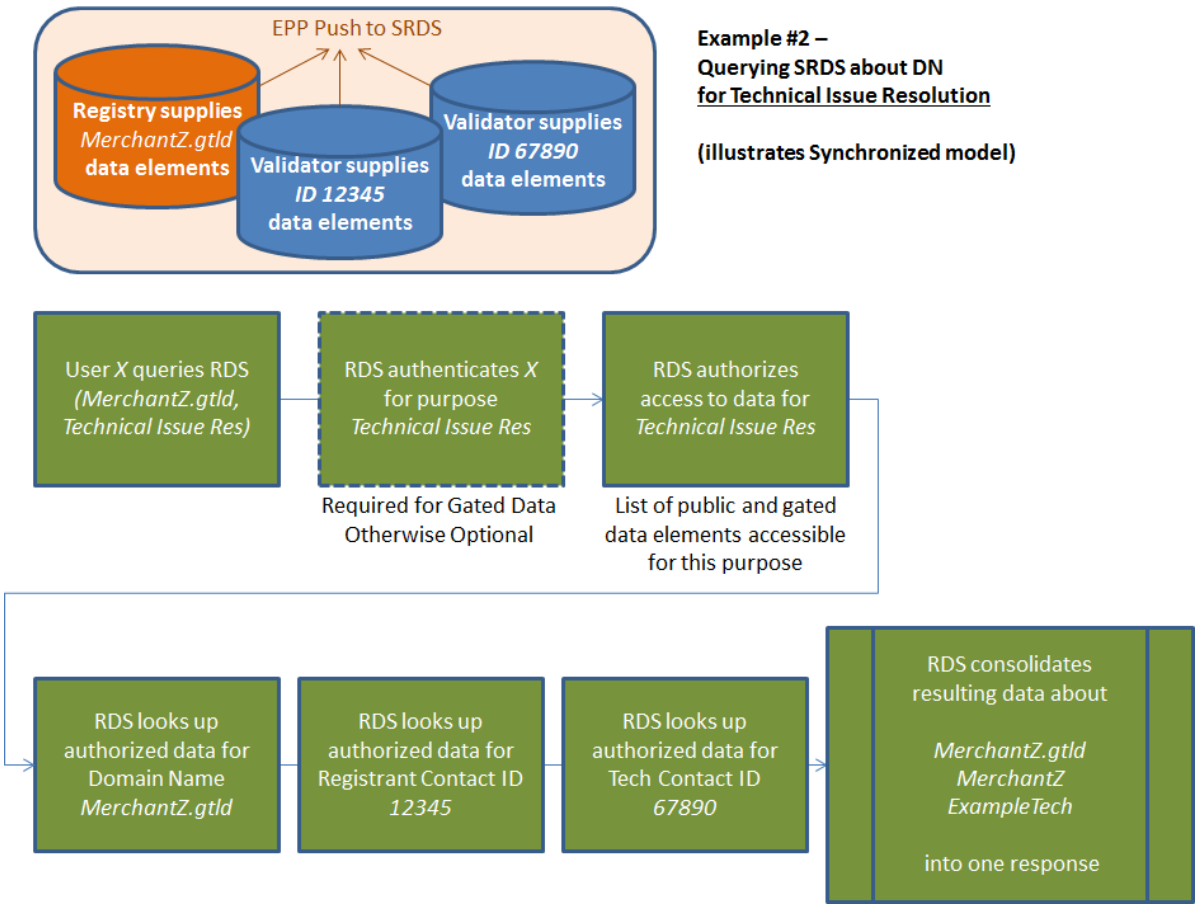
Note that the processes described above do not address when a proxy or privacy registration must be "unmasked" to the public rather than simply "revealed" to the requestor.

These suggested models and processes must be further refined by the GNSO PPSAI WG, based upon their consideration of ICANN community needs and informed by best practices identified by responses to the EWG's on-line survey of Privacy and Proxy Service Providers.

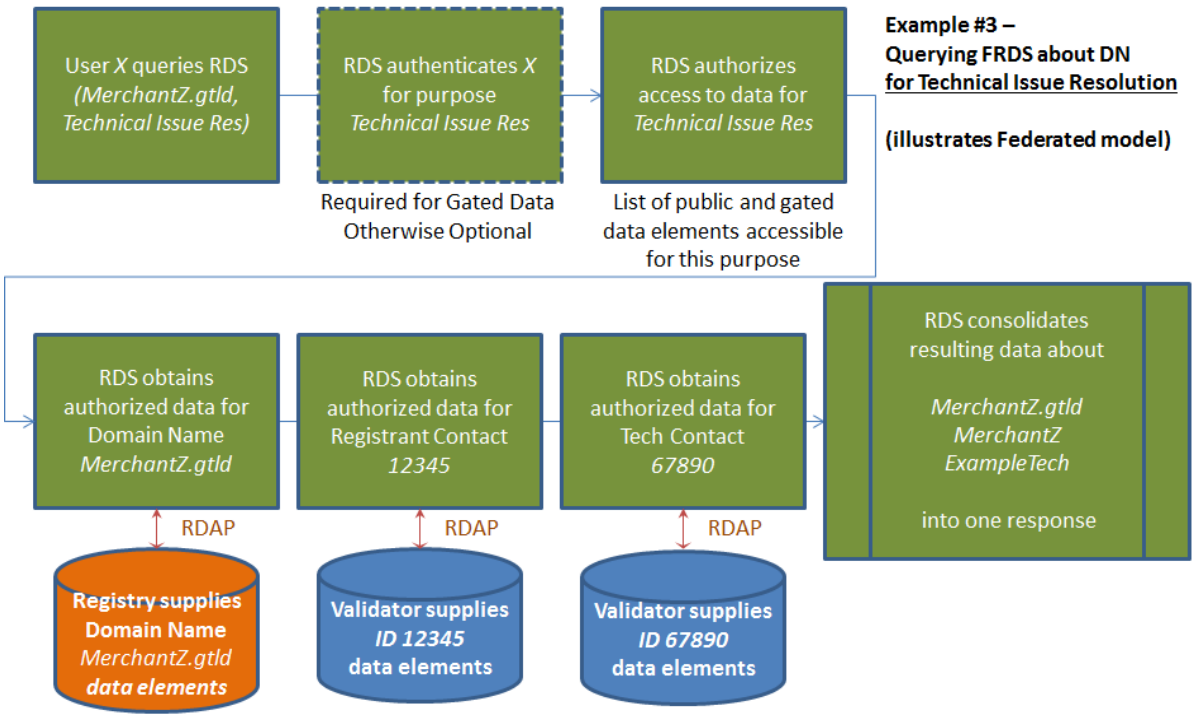
ANNEX I: RDS PROCESS FLOW CHARTS

The following flow charts illustrate key data flows between RDS ecosystem actors during domain name registration and requestors querying the RDS for information about that domain name for technical issue resolution.





To facilitate model comparison, this same example is repeated below for the FRDS.



ANNEX J: ABOUT THE EWG

Selection Process & Vision

In convening the EWG, the ICANN Board adopted a novel approach to resolving a difficult issue that has been plagued by stalemate and divisiveness in the past. The Board brought together individuals representing a wide range of perspectives and stakeholders in the hope that by sharing their expertise, they could succeed where others had failed. With the delivery of this Final Report and its 180 consensus-supported principles, the Board's vision has indeed materialized.

The members of the EWG were carefully selected with the assistance of a seasoned and neutral facilitator, Jean-Francois Baril. He was chosen because of his experience in developing standards in the consumer electronics industry. Dozens of EWG applicants were screened based on several criteria, including leadership skills, expertise, geographic diversity, consensus building, aptitude to innovate, and in some cases, neutrality. It was felt that individuals from outside the ICANN community could bring a fresh perspective, one unjaded by past attempts to address the WHOIS issue.

Composition of the EWG

The EWG membership consists of individuals, Board liaisons and Staff from Australia, Canada, China, the European Commission, Ireland, Jamaica, Nigeria, Norway, Switzerland, the United Kingdom, and the United States. This geographic diversity proved instrumental to understanding the many jurisdictional challenges associated with the EWG's work.

Among the EWG members were seasoned entrepreneurs and global leaders (Ajayi, Ala-Pietilä, Neylon, Rasmussen, and Shah). Their collective expertise in balancing risks and their results-oriented problem solving style paved the way to reaching an early consensus among the EWG.

Because the EWG mandate included examination of public policy, notably privacy issues, specific expertise in the government sector was key to its success. Perrin and Niebel contributed experience from a Canadian and European perspective, ensuring that these issues were in the forefront of the design of the next-generation system. It is significant that during its deliberations, the EWG was apprised of, and tried to be mindful of, recent developments in the European Union data protection legislation.

Another critical aspect of the EWG's work included ensuring that its recommendations were reasonably implementable in today's DNS ecosystem. Expertise from gTLD Registrar (Neylon), gTLD Registry (Hollenbeck-.com and .net), and the ccTLDs (.cn-Jian, .uk-Nanayakkara, .ng- Ajayi and .au-Disspain) members shed light on issues such as validation approaches, Privacy/Proxy registrations, compatibility with protocols such as EPP and the new RDAP being developed at the IETF, as well as incorporation of concepts such as "gated access" for the display of sensitive data elements.

Security and stability issues were also examined, capitalizing on the insight of present and former members of SSAC (Crocker and Rasmussen), contributing their vast understanding of law enforcement needs in combatting malicious abuse involving the DNS.

Design of a new system is impossible without considering the needs of the many users of the next-generation RDS. The EWG included members with deep knowledge of the intellectual property issues (Kawaguchi, Vayra, and Shah) that rely heavily on the current WHOIS system to combat cybersquatting, fraud, and online counterfeit, as well as insights shared by end-users (Samuels and Phifer). These varied perspectives helped ensure that legitimate purposes for RDS access to registration data would be accommodated, while minimizing the inefficiencies and abuses of the current registration processes wherever possible.

To supplement the EWG, ICANN staff members (Michel, Milam) brought executive insight and knowledge of ICANN's contractual framework. A consultant (Phifer) also provided data from the extensive GNSO WHOIS studies conducted over the last five years to help the EWG formulate fact-based recommendations.

Working Methodology

The EWG kicked off its work with a series of getting-to-know each other activities intended to build rapport, trust, and most importantly, a sense of belonging to a team. The EWG established a set of team values to overcome any obstacles to exploring innovative solutions for this complex problem. These are:

- On this Team as individuals
- Speak freely
- No social media attribution
- Intellectual honesty
- Industry self-regulation
- Design afresh
- Factor in hard realities (technology and governments)

These values helped guide the EWG to the compromises necessary to design the RDS and produce the principles outlined in this Final Report.

For more information and the biographies of EWG members, please see this announcement.