Status Update Report from the Expert Working Group on gTLD Directory Services: A Next Generation Registration Directory Service

STATUS OF THIS DOCUMENT

This is an update from the Expert Working Group on gTLD Directory Services (EWG) describing the progress made since our initial report on recommendations for a next generation registration directory service (RDS) to replace the current WHOIS system.

I. EXECUTIVE SUMMARY

This Status Report highlights the EWG's current thinking with respect to several key issues that were raised by the Community in reaction to its Initial Report. As its deliberations are still on-going, it is hoped that this explanation will stimulate lively Community discussion and dialogue at the ICANN-48 Meeting in Buenos Aires.

Some of the key issues highlighted in this Status Report are:

- Identification of the data elements to be freely available on an anonymous basis, and those that may require access through accreditation and a permissible purpose.

  In the Initial Report, the EWG introduced its recommendations for a new Registration Data Service (RDS) whereby some data elements might be disclosed for permissible purposes only to authenticated requesters (referred to as "gated access"), while other less sensitive data elements could continue to be accessed in a manner similar to today's WHOIS (free, publicly available & anonymous). This Status Report identifies each data element that the EWG suggests be collected and stored in the RDS, and whether such data element would be available through public access or gated access In addition, **Annex A** includes a detailed illustration of data elements returned in response to an anonymous public data query, as well as those returned in response to a query requiring gated access.

- Details on the principles for a better privacy service and a proposal for secured protected credentials.

  The EWG suggests adoption of an "Enhanced Protected Registration Service" for general personal data protection and adherence to local privacy law, to address well-documented shortcomings in today's privacy (renamed "Shield") services and proxy services. To address both domain name registrant and stakeholder

needs for more uniform and reliable Shield and Proxy Services which enable greater accountability, a series of principles and processes are highlighted in this Status Report.

With increasing demands for a responsive, accurate directory, with more discipline in the accreditation and procedures applying to proxy and shield services, it will be also be important to protect the vulnerable. The EWG suggests creation of a "Maximum Protected Registration Service" that offers Secured Protected Credentials Service for at-risk, free-speech uses. This service would safeguard those who most need to use the Internet for the purposes of free speech and communication within groups, while providing remedies for abuse. The EWG suggestion would establish procedures for the enablement of vulnerable and disadvantaged groups to benefit from the many advantages of holding their own domains on the Internet.

- <u>Exploration of how technical protocols could be deployed in the recommended models.</u>

  The EWG examined whether the technical protocols deployed in today's domain registration system (such as EPP), and under development in the IETF (such as by the WEIRDs working group), could support the design features recommended by the EWG. The EWG's initial analysis suggests that both EPP and RDAP (under development by the WEIRDs working group) protocols can be used by the RDS, no matter which of the two top system design models is chosen, with some extensions, additions, or modifications.

- <u>Comparison of the current WHOIS system (as improved in the 2013 RAA) to the EWG recommended model</u>

  Recognizing that the current WHOIS system has recently been improved through the adoption of new agreements (most notably, the 2013 Registrar Accreditation Agreement (2013 RAA) and the New GTLD Registry Agreements), the EWG tested the improved WHOIS against its set of design features and principles desirable for the next generation registration directory services. 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, including:

- Anonymous public access creates an environment where mining and abuse can occur, with little accountability or ability to remedy
- Limited ability to protect the privacy of individuals
- Limited ability to ensure integrity of registration data; registrants can easily insert false contact details, including those held by another
- Lack of Security Features
- Lack of auditing capabilities
- Limited ability to apply different rules to conform to differing data privacy regimes
- Unacceptable accuracy levels creates inefficiencies for those seeking to communicate with registrants

These are just a few of the deficiencies described below in Section IV.h.

- Description of the various system models examined by the EWG, and a comparison of the pro/cons of the top two models.

  The EWG recognizes that the Initial Report did not provide sufficient detail for the Community to understand the process of analysis it conducted to reach its recommendations for the proposed Aggregated Registration Data Service (ARDS). This Status Report provides additional details about several alternative models explored by the EWG in preparing its Initial Report, and the work undertaken since Durban to test and deepen its analysis.

  The EWG identified two top system models to further analyse and compare- the ARDS recommended in the Initial Report, and the "federated model," which differs in that the registration data is stored and controlled by the gTLD registries rather than by the ARDS.

  After comparing these possible models, the EWG observed that except for the current Whois, all are capable of satisfying the proposed RDS principles to some degree.

The principles and issues discussed below are works-in progress and should not be interpreted as consensus recommendations. As part of its work plan, the EWG will pursue research in specific areas to facilitate fact-based findings for its Final Report.[1]

II. EWG Purpose & Initial Report Publication

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[2] published during this period point to deficiencies in the current system that call 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.

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 (too 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

[1] See Section V for details on the specific research to be conducted.

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

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 an Aggregated RDS (ARDS) model[3] that might be capable of collecting and disclosing accurate domain name registration data elements for permissible purposes.

The EWG's Initial Report enumerated the users, purposes, data elements, recommended principles and features, and proposed model. This initial report on work in-progress was accompanied by a questionnaire soliciting community input on complex areas needing further analysis to draft consensus recommendations. While comments were received on the entire initial report, two topics received the most feedback: the EWG's recommendation to replace anonymous WHOIS with a gated access paradigm, and the suggested ARDS implementation model.

This Status Report aims to highlight the EWG's current thinking on these and many other key issues, after careful consideration of all comments and feedback received to date. It also provides a great deal more detail on the analysis that lay behind the Initial Report, as requested by the community.

III. Progress since the Initial Report

The EWG has engaged in a detailed analysis of the feedback received on its Initial Report, using the Community's extensive and diverse input to inform its on-going work

[3] For further description of initial ARDS, please refer to Section V of the Initial Report.

on open areas and to test and refine its initial 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 has not yet completed its recommendations, but intends to do so in early 2014.

a. Community Input on the Initial Report

The EWG's Initial Report (published on 24 June, 2013) generated 35 public comment submissions and over 100 online questionnaire responses from the ICANN Community, reflecting both the continued interest and diversity of stakeholder opinions on an issue that has been controversial for over a decade. This diversity reinforces the difficulty of the task assigned to the EWG, and the need for the EWG to produce recommendations that, while not perfectly satisfying every stakeholder's needs, describes a next-generation RDS that better addresses those needs than the current WHOIS system.

The EWG thanks the ICANN Community for the meaningful comments and feedback on its Initial Report. After careful consideration of each submission, the EWG has produced a Summary Response to Public Comments. The EWG used these written comments and other Durban meeting and online inputs to pinpoint where clarifications were needed, where concerns should be investigated, and where alternatives should be considered. The EWG has updated its initial work and proposals still under development to reflect this input; many of those areas are discussed in greater detail in this Status Report.

b. Interaction with subject matter experts and stakeholders

Several commentators encouraged the EWG to consult with subject matter experts to ensure that its recommendations are fact-based and reasonably implementable. While the EWG had solicited this input at the ICANN Beijing meeting and in other consultations prior to publishing its Initial Report, the EWG further expanded this outreach in Durban and after, by meeting with numerous subject matter experts and stakeholder groups.

- Stakeholder sessions were held with the GNSO, RrSG, CSG, NPOC, IPC, GAC, and NCSG. Slides, audio archives and/or transcripts of each Durban public or stakeholder meeting session can be found at this page.
- The EWG also received briefings from subject matter experts, including representatives from several law enforcement organizations, the Internet and Jurisdiction Project director Bertrand de La Chapelle, the Centralized Zone Data Access Program, and the Secure Domain Foundation.

The complexity of matters to be considered ultimately led the EWG to recommend that deeper investigation be conducted on 5 specific topics (enumerated in Section V) before finalizing its recommendations to the ICANN Board.

IV. Update on Progress in Open Areas

The proposals described in this Section reflect the progress made by the EWG with regard to areas identified as needing further consideration in the Initial Report. Note, however, that these proposals remain a work-in-progress, incomplete but shared in this Status Report to enable a richer discussion with the ICANN Community in Buenos Aires. Please note that these proposals are not yet consensus recommendations by the EWG.

a. Improving Accountability

The proposed 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.

As stated in its Initial Report, 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 anonymous access to public data elements, with 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 comments raised concerns about abandoning entirely anonymous public WHOIS in favor of the proposed gated access paradigm. Some comments 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, the EWG has continued its consideration of purpose-driven access to public and gated data elements. This Section elaborates on the EWG's recent work in these areas.

Proposed Categorization of Data Elements (Public/Gated)

In addition to principles included in the Initial Report, the group has developed the following principles to categorize data elements to be collected and disclosed.

Step 1: DATA COLLECTION

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

No.	Principles for Data Collection
1.	To meet basic domain control needs, it should be mandatory for Registries and Registrars to collect and Registrants to provide the following data elements when a domain name is registered; this data would not necessarily all be sent to the RDS: a. Domain Name b. DNS Servers c. Registrant Name d. Registrant Type Indicates the kind of entity identified by Registrant Name: natural person, legal person, proxy service provider, trusted agent e. Registrant Contact ID A unique ID assigned to each Registrant Contact [Name+Address] during validation (refer to Section IV.b., for a more detailed definition of Contact ID and how it is created and used) f. Registrant Postal Address Includes the following data elements: Street, City, State/Province, Postal Code, Country (as applicable) g. Registrant Email Address Registrant Telephone Number Includes the following data elements: Number, Extension (when applicable)
2.	To avoid collecting more data than necessary, all other Registrant-supplied data used for at least one[4] permissible purpose should be optionally provided at the Registrant's discretion. Registries and Registrars must allow for this data to be collected and stored if the Registrant so chooses.
3.	To maximize Internet stability, the following mandatory data elements should 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

[4] The EWG is considering whether this should be one permissible purpose or two permissible purposes.

	i. Registrar Expiry Date j. Updated Date k. Registrar URL l. Registrar IANA Number m. Registrar Abuse Contact Phone Number n. URL of Internic Complaint Site
4.	For TLD-specific data elements, the TLD operator should establish and publish a data collection policy (consistent with these over-arching principles) and be responsible for any validation of those TLD-specific data elements.
5.	Registries and Registrars may collect, store, or disclose additional data elements for internal use between the Registrar and Registrant, but never shared with the RDS.[5]

Step 2: DATA DISCLOSURE

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

No.	Data Disclosure Principles
1.	To maximize Registrant privacy, Registrant-supplied data should 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, except as noted due to high risk.
2.	To maximize Internet stability, all Registry or Registrar-supplied registration data should 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.
3.	To maximize reachability, all optional role-based contacts should be public by default. • Registrants can opt into making any public contact gated.
4.	To meet basic domain control needs, the following Registrant-supplied data which is mandatory to collect and low risk to disclose should be included in the minimum public data set:

[5] 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.

	a. Domain Name b. DNS Servers c. Registrant Type d. Registrant Contact ID (further defined in Section d) e. Registrant Email Address *(note: Tel# is mandatory to collect but not to disclose)*
5.	For TLD-specific data elements, the TLD operator should 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.

ALIGNMENT WITH 2013 RAA

To facilitate transition and understanding, EWG-proposed data element names have been aligned with those identified in the 2013 RAA where intended definitions appear to be equivalent:

RDS DNSSEC Keys -> RAA DNSSEC Delegation
RDS Expiry Date -> RAA Registrar Expiry Date

However, data element names used in the 2013 RAA for contact data elements cannot be used to convey the EWG's proposal for role-based contacts (see Section IV.b.) To cover this, the EWG applied the following mappings:

When RDS Contact Role = Admin,

RDS Contact Name = RAA Admin Contact Name

RDS Contact Organization = Admin Contact Organization

and so forth for other RAA Admin Contact data elements

When RDS Contact Role = Tech,

RDS Contact Name = Tech Contact Name

RDS Contact Organization = Tech Contact Organization

and so forth for other RAA Tech Contact data elements

The EWG relied upon the 2013 RAA to define all existing data elements, detailing only differences or necessary clarifications. For proposed data elements NOT identified in the 2013 RAA, the EWG will include definitions in its final report, along with examples and

rationale for adding them. The EWG will also note certain data elements which pose transition and compliance challenges needing further investigation.

DOMAIN NAME PURPOSE

After considerable discussion, the EWG has re-evaluated its initial recommendation to include Domain Name Purpose as a data element collected and disclosed by the RDS. Instead, the EWG is considering additional principles to accomplish associated goals. For example, when registering/updating a domain name, any Legal Person Registrant might be encouraged to make all Gated-by-Default data elements public. This might have the result of 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.

RESULTING DATA CLASSIFICATIONS

Based on these new principles, the following table details the resulting classification for each RDS data element now being considered 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 and provided by Registrants, while
  (O)ptional means data must be requested by the Registrar but may or may not be provided at the Registrant' s discretion, as applicable.

  [2] 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 [anonymously accessible to everyone] or (G)ated [accessible to authenticated users, for permissible purposes only]. This means:

[3] For data collected from Registrants,

P ■☐ G means any data collected must be public and cannot be hidden,

P ☒☐ G means any data collected is public by default but can be hidden by Registrant,

P☐☒ G means any data collected is gated by default but can be made public by Registrant, and

P ☐■ G means any data collected must be gated and cannot be disclosed without gating

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

P ■☐ G means any data provided must be public and cannot be hidden, while

P ☐■ G would mean any data provided must be gated; no date elements fall into this category.

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.

	Collection M or O	Disclosure P or G	In RAA?	Notes
REGISTRY/REGISTRAR PROVIDED DATA				See [2] Collection Definition and [4] Disclosure Definition
Registration Status	**M**	P ■☐ G		
DNSSEC Delegation	O	P ■☐ G		Renamed to align
Client Status (Registrar)	**M**	P ■☐ G		
Server Status (Registry)	**M**	P ■☐ G		
Registrar	**M**	P ■☐ G		
Reseller	O	P ■☐ G		
Registrar Jurisdiction	**M**	P ■☐ G	**New**	
Registry Jursidiction	**M**	P ■☐ G	**New**	
Reg Agreement Language	**M**	P ■☐ G	**New**	
Creation Date	**M**	P ■☐ G		
Original Registration Date	O	P ■☐ G	**New**	
Registrar Expiry Date	**M**	P ■☐ G		Renamed to align
Updated Date	**M**	P ■☐ G		Renamed to align
Registrar URL	**M**	P ■☐ G		Added to align
Registrar IANA Number	**M**	P ■☐ G		Added to align
Registrar Abuse Contact Email Address	**M**	P ■☐ G		Added to align
Registrar Abuse Contact	**M**	P ■☐ G		Added to align

	Collection M or O	Disclosure P or G	In RAA?	Notes
Phone Number				
URL of Internic Complaint Site	**M**	P ■☐ G		Added to align
REGISTRANT DATA collected from Registrant				See [1] Collection Definition and [3] Disclosure Definition
Domain Name	**M**	P ■☐ G		
DNS Servers	**M**	P ■☐ G		
Registrant Name	**M**	P☐☒ G		
Registrant Type	**M**	P ■☐ G		
Registrant Contact ID	**M**	P ■☐ G	**Replace**	Replaces Registry Registrant ID, issued by Validator in RDS
Registrant Organization	O	P ☒☐ G		
Registrant Company Identifier (e.g., Trading Name, D-U-N-S)	O	P ☒☐ G	**New**	Real-world identifiers issued to businesses by sources such as Dunn and Bradstreet
Registrant Street Address	**M**	P ☐☒ G		Expanded to align
Registrant City	**M**	P ☐☒ G		"
Registrant State/Province	O	P ☐☒ G		"
Registrant Postal Code	**M**	P ☐☒ G		"
Registrant Country	**M**	P ☐☒ G		"
Registrant Phone + Ext	**M**	P ☐☒ G		Extension if applicable
Registrant Email Address	**M**	P ■☐ G		
Registrant Fax + Ext	O	P ☐☒ G		
Registrant SMS/IM/Other	O	P ☐☒ G	**New**	Extension if applicable
ROLE-BASED CONTACTS IF supplied by Registrant	**If contact is supplied…**			See [1] Collection Definition and [3] Disclosure Definition
Contact Name	**M**	P ☒☐ G	**?**	Person's name or role?
Contact Role	**M**	P ☒☐ G	**New**	
Contact ID	**M**	P ☒☐ G	**Replace**	Replaces Admin/Tech Registry ID
Contact Organization	O	P ☒☐ G		
Contact Street Address	O	P ☒☐ G		Expanded to align
Contact City	O	P ☒☐ G		"
Contact State/Province	O	P ☒☐ G		"
Contact Postal Code	O	P ☒☐ G		"
Contact Country	O	P ☒☐ G		"
Contact Phone + Ext	O	P ☒☐ G		Extension if applicable
Contact Email Address	O	P ☒☐ G		
Contact Fax + Ext	O	P ☒☐ G		Extension if applicable
Contact SMS/IM/Etc	O	P ☒☐ G	**New**	

DATA DEFINITIONS [initial definitions given for discussion]

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.[6]
- **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.
- **Registrant Contact ID:** A unique handle assigned to a pre-verified contact identified as this domain name's Registrant. Refer to Section IV.b., 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.
- **Registrant SMS/IM/Other:** An address that may be used to reach the Registrant via SMS, instant messaging, or another alternative communication vector.
- **Contact Role:** The role played by this contact (e.g., technical, administrative, etc).
- **Contact ID:** A unique handle assigned to a pre-verified contact identified as a contact for this domain name, in the role indicated by the Contact Role. Any role-based Contact ID may or may not be the same as the Registrant Contact ID.

The EWG is still considering proposals to make additional data mandatory to collect and/or public to disclose when Registrant Type is Legal Person or Proxy Provider. It is also considering whether to collect a "Registrant Initial Registration Date" to capture the date when the current registrant first registered the domain name. The EWG also reiterates its recommendation to perform a widely scoped risk/impact analysis to

[6] This is different than the creation date since the creation date picks up the latest time that the domain name was registered, but 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.

confirm that these principle-based classifications do in fact result in appropriate collection and disclosure of data for defined purposes.

Proposed User Accreditation for access to Gated Data

The EWG consulted with Europol, Interpol, and other members of the global Law Enforcement community to assess possible accreditation models and bodies. As part of this consultation, the EWG developed a deeper understanding of WHOIS data currently used in criminal and civil investigations, and intends to map this feedback to use cases where data needs differ.

In addition, the EWG has recommended that, for each RDS User desiring access to gated data for permissible purposes, experts should be consulted to identify possible accreditation bodies. As part of this consultation, the EWG expects to review use cases to confirm and better identify what data is needed for various purposes (e.g., brand owners and agents, or Op Sec personnel investigating problems or abuses).

Following further investigation with subject matter experts and public comments about RDS user accreditation for access to gated data, the EWG has drafted the following additional principles, now under discussion:

No.	Additional Gated Access Principles
1.	There should be a non-accredited, anonymous, access method to non-gated data in real-time.
2.	The RDS should only apply the minimum "accreditation scheme" necessary to provide access for the stated purpose.[7]
3.	There should be no need 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 accreditation.
4.	Accreditation for access to data could be granted in four ways/players: • None (anonymous access as above) • Self-accreditation by the person/entity requesting the data (system

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

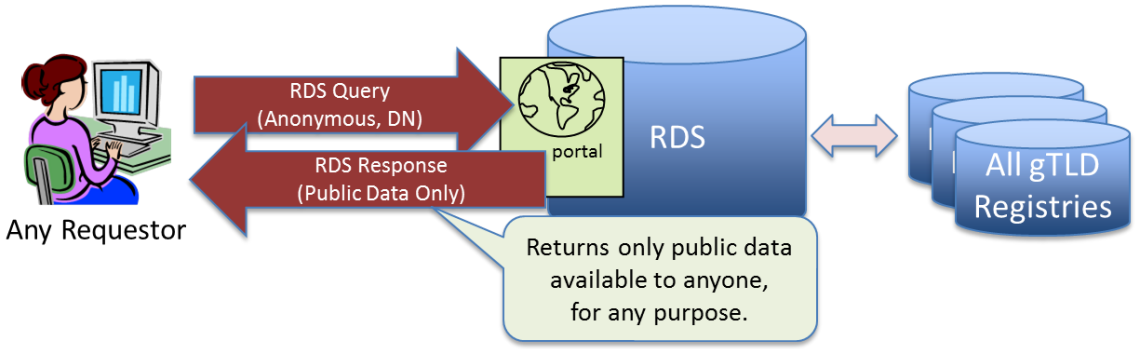
	where the user simply states who they are, perhaps via a standing "account" and what they are requesting and why, and then are granted access to that level of data gives you) – standing account could be used for this. • Accreditation by the subject of the data via a request process (e.g. the person looking up domain requests access for a given purpose, and the subject of that data request grants it) • Some trusted third party
5.	Whenever possible, any third-party RDS accreditation process should leverage existing accreditation processes within a user community identified as one that would need credentialing.
6.	These third-party accreditation processes should be vetted by some authority TBD (for example, ICANN, RDS, panel, etc.) and reviewed on a periodic basis.
7.	Any organization administering them should have a signed agreement with ICANN and/or the RDS to operate such accreditation processes under agreed-upon guidelines and a framework to allow for due process, accountability, security, fair access, and adherence to applicable law.
8.	An organization could apply for accreditation and have all people using the RDS in their organization covered by that one accreditation.[8]
9.	The RDS should be flexible enough to allow creation of both organization-wide and individual credentials for non-anonymous access.
10.	Supplying accreditation for access of RDS data does not have to happen in real-time for all use cases and/or requesters.[9]
11.	The RDS should accommodate automation for large-scale lookups for various use cases and purposes.[10]
12	A single requestor playing different roles may have multiple credentials in order to access different types of data. Within a single role, only one credential should be possible.
13.	Audits and data analytics should be used to identify abuse of the system and access credentials.

[8] It is up to the organization to ensure the integrity of any issued credentials for accessing the RDS.
[9] This allows for both a "registrant approval" or verification process to kick off based on the location of the requestor.
[10] For example, registration data on domains detected hosting malicious content are routinely pulled in via automated processes. This will in-turn populate investigatory tools, kick-off notification processes, and/or provide input into other lookups that attempt to identify malicious infrastructure.

Illustration of Public Data Access

As depicted in the following figure, public data elements can still be requested anonymously via the RDS. Refer to **Annex A** for more detailed illustration of data elements returned to an anonymous public data query.

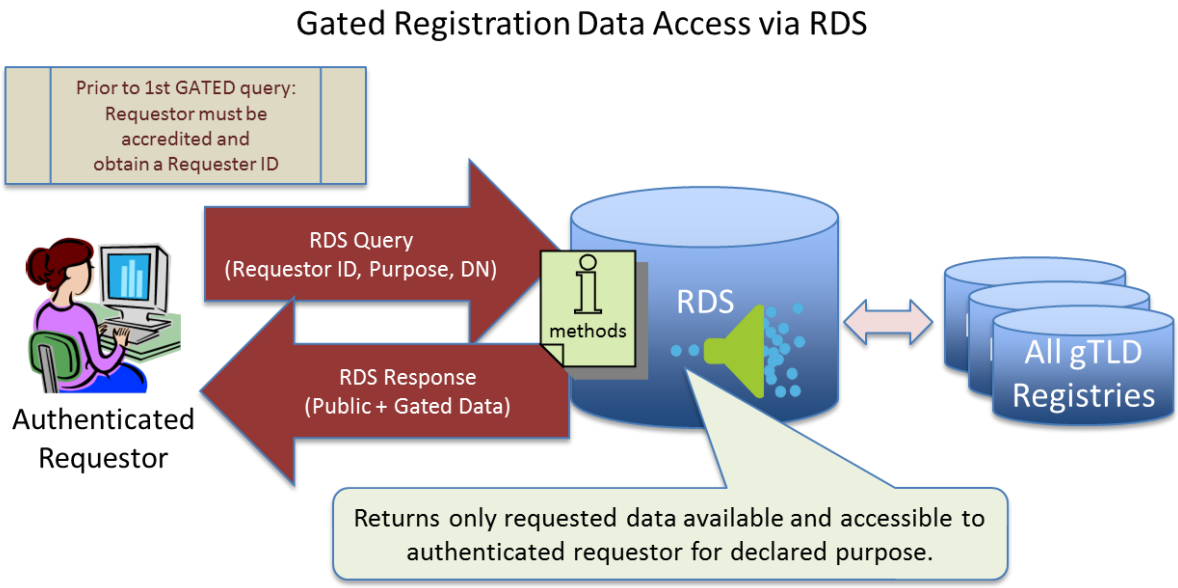
Anonymous Public Registration Data Access via RDS



Annex A also contains 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 A** for more detailed illustration of data elements returned to an authenticated gated data query.



Summary of Key Benefits

By incorporating an accreditation regime for gated access to data elements, the RDS enables:

- Greater data accuracy due to protection of sensitive data elements from public display leading to sharing of more accurate data by registrants.
- Providing a supporting framework to address data protection legislation in varied jurisdictions (limited access by purpose and auditing).
- Establishing a method to provide accountability for people accessing data for varied purposes.
- Enabling improved access capabilities to improve overall efficiency of the "system."

b. Improving Data Quality

As stated in its Initial Report, the EWG proposes 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. In addition, 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.

To accomplish this, the Initial Report proposed that the RDS 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 registrant contact data for reuse in multiple domain name registrations. At the time of Initial Report publication, the EWG was still working to flesh out the details of validation and related processes.

Many comments received on this topic requested further detail regarding validation processes and related interactions between the RDS, Registrars, and Registries. A number also sought comparison with accuracy improvements promised by the 2013 RAA and related ICANN initiatives to implement WHOIS Review Team recommendations.

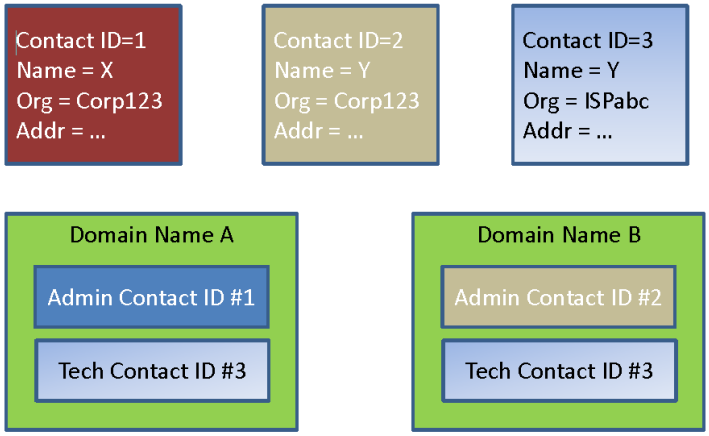
The EWG's work continues to evolve in this area; the group is currently considering a new proposal for a pre-validated Contact Directory that might promote the quality and reusability of data elements used to contact domain name registrants. Draft principles and processes now under discussion by the EWG are further detailed below.

Proposed Contact Management and Validation Process

Pre-validation of registrant or other contact information is desired to satisfy the following purposes:

- Increase accuracy of contact information by utilizing pre-validated contact information: checking of data prior to use for a new domain name and consistent data across all registrations (reduces error and fraud)
- Avoiding the need to validate registrant data each time a registrant registers a new domain name. Validation is performed once, and can then be used for several domain registrations.
- To 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).

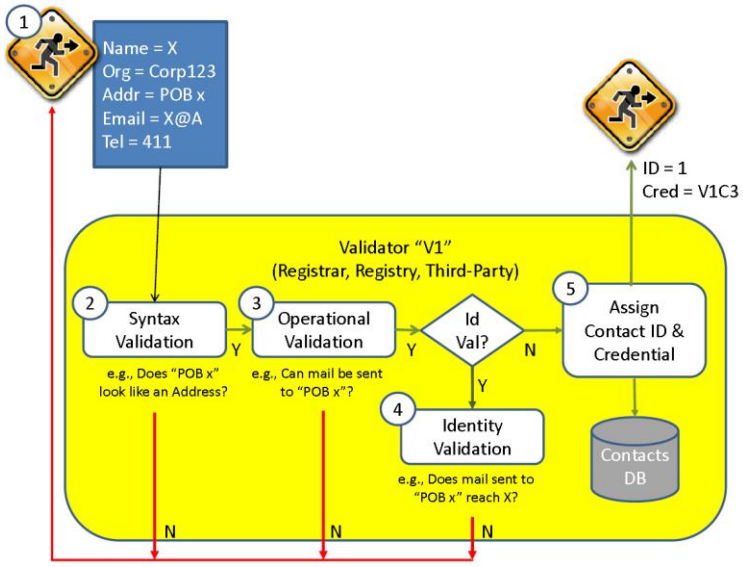


Updates made to Contact ID #3 automatically reflected in Data for Domain Names A and B

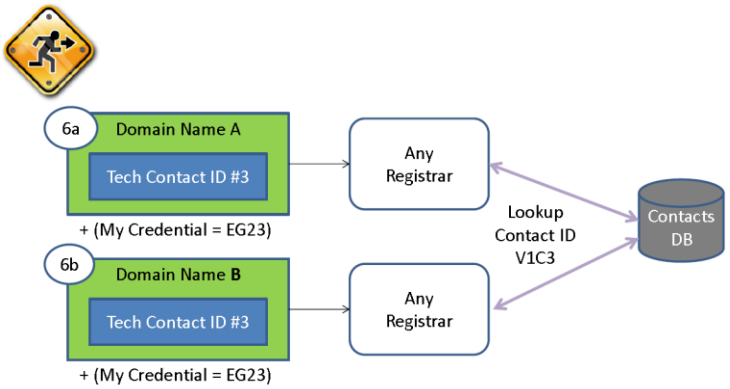
To address these needs, the following pre-validation process may be recommended:

- Applicant submits contact data through validator of his or her choice (e.g. registrar, registry, accredited 3rd party contact management provider) to the RDS
- Syntactic and operational validation (per SAC-058) are carried out by Validator

- **Optional**:[11] Identity validation to be carried out by the Validators who may utilize entities like post offices, ccTLD managers, Telephone companies, tax offices etc.
- After a successful syntactic validation, a unique identifier is issued to the validator by the RDS
- The validator issues credentials (as applicable) and relays unique identifier to the applicant
- The applicant proceeds to any registrar, using his unique identifier, to register domain names
- Pre-validated unique identifiers can be utilized for any particular contact role for a domain name (tech, admin, billing, abuse, legal or whatever is provided in the model employed)

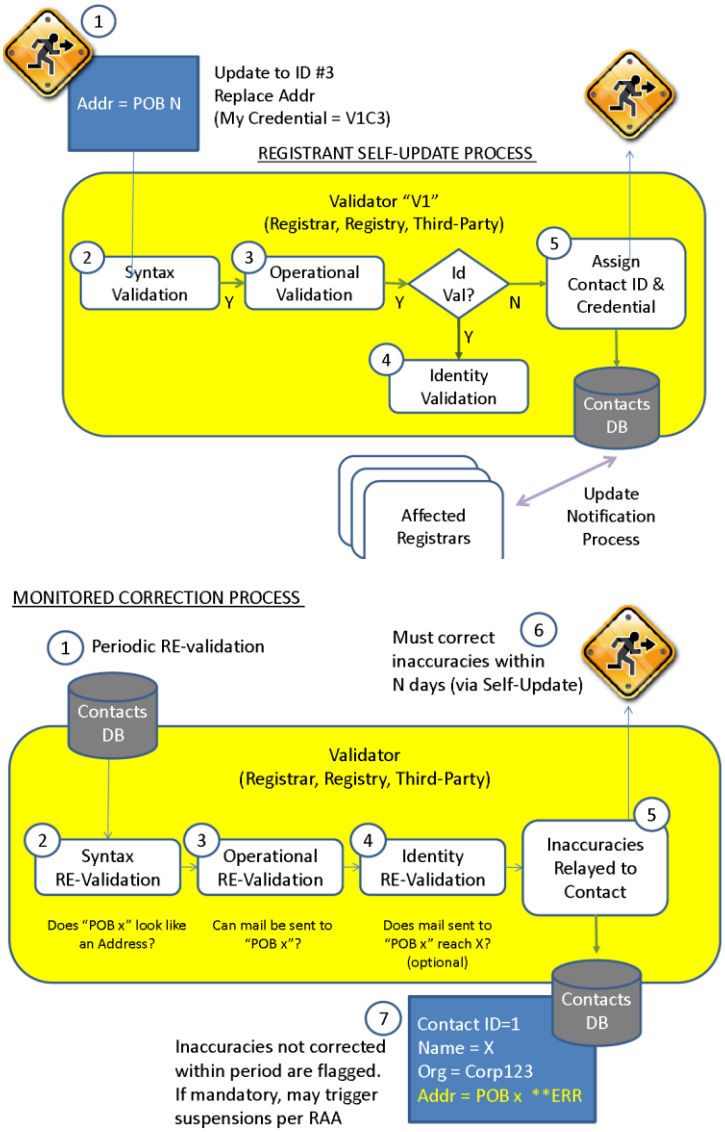


[11] The EWG is evaluating whether this should be optional or mandatory.



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

- **Self-correction**: Unique identifier holder uses allowed Validator to correct /update their contact data using their previously issued credentials – information automatically flows across to all domains utilizing that particular contact information (as designated by the unique ID)
- **Monitored process**: Validators conduct periodic operational and identity validation on contact sets managed via their service.
- Inaccurate data is reported to the Unique Identifier holder, such holders are given a specific period of time, for example 14 days, to correct the inaccuracy. Registrants, registries, and registrars of any affected domains may be notified. Unique identifier holder uses any authorized validator to correct the inaccuracy using their previously issued credentials.
- If the registration data remains inaccurate after the deadline, the data is flagged as inaccurate. If the flagged data is mandatory, then the associated domains are put into a remediation process that may include suspension per the applicable RAA.
- Once the flagged data is replaced with valid data, any sanctions are removed from affected domains.



Proposed Data Element Validation Principles

In addition to the validation principles proposed by the Initial Report, the group is discussing the following new principles:

No.	Principles Related to Contact IDs
1.	In order to promote better accuracy, ease-of-use, and consistency of process, individuals, unique contact identifiers (Contact IDs) associated to specific sets of contact data should be issued to organizations, and other entities that publish "contact data" used for registry services. [12]
2.	Contact IDs are associated with discreet blocks of contact information necessary to play a role in a domain name registration.
3.	Contact IDs are issued by via accredited entities (e.g. registrars, registries, and third party validation providers) – referred to as Validators.
4.	In order be associated with a domain in any contact role, one must have an assigned Contact ID.
5.	Contact IDs can be assigned to multiple roles for one or many domains. E.g. registrant for one domain, technical and abuse contact with other domains.
6.	Contact IDs can be created as part of the domain registration process.
7.	A Contact ID can be validated at three different levels, syntactic, operational, and identity as per SAC 058.
8.	Validators can offer multiple levels of authentication for Contact Holders to utilize at their discretion, allowing for differing rigor to utilize or modify contact information for a particular Contact ID.
9.	Contact Holders may choose the level of authentication they desire to allow changes ranging from "none" to "high." [13]
10.	In order to preserve associations, a Contact ID can have a status of "inaccurate" and remain in the system.
11.	Active domains cannot have a mandatory contact with an "inaccurate" status without some sort of remediation, up to and including suspension.
12.	All data elements of contact data for a Contact ID must be validated at a syntactic level.
13.	Mandatory data elements for a contact identifier must be validated operationally prior to use of that Contact ID for a role related to a domain name.[14]
14.	A Contact Holder may seek higher levels of validation (e.g. fully validated at the identity level) than minimum requirements dictate on a voluntary basis. [15]

[12] Such entities are "Contact Holders".
[13] For example, for a "high" authentication designation, multi-factor authentication may be necessary to access and change data associated with a Contact ID.
[14] More stringent option: The mandatory data elements for a Contact ID must be validated operationally and at least one primary contact data element be identity validated prior to use of that Contact ID for a role related to a domain name.
[15] This is akin to an EV CERT vs. a standard CERT in the CERT model. Rationale – an entity performing commerce or other sensitive transactions can increase consumer trust with higher levels of validation.

15.	A minimum level of cross-field validation should be designated and routinely checked for all contacts.
16.	At a minimum, X[16] fields should be cross-field validated at the operational level meeting the applicable RAA.
17.	Revalidation of contact data should be carried out on a regular basis by the applicable validator. [17]
18.	Given the probable costs involved with identity validation, it is desirable to create a mechanism for economically disadvantaged applicants to receive identity validation.
19.	Validation Status of the Contact ID should be tracked and published as appropriate when accessing RDS information.[18]
20.	If a Contact Holder provides optional information for collection, it must be at least syntactically and operationally validated.
21.	For any given contact identifier, a Contact Holder may choose any particular Validator. [19]
22.	Oversight and accountability policies related to the management of the Contact IDs would need to be developed.[20]
23.	Changes to the contact data for a Contact ID must be made by the Contact Holder via the currently designated Validator. [21]
24.	In order to combat impersonation, defamation, and abuse, a Contact Holder may designate that their contact data is unique and should not be used by other Contact Holder claimants. [22]

[16] The minimum number of fields to be validated is under discussion.
[17] For example, Syntactical validation should be carried out on at least an X interval, and operational validation should be carried out on at least a Y interval. If identity validation has been confirmed, then it should be rechecked on at least a Z interval. X, Y, and Z TBD.
[18] These values may include the following Statuses:

- Inaccurate
- Syntactically valid
- Operational valid
- Identity valid (verified)
- Unique

[19] Additional implementation processes would be needed to enable the contact holder to update that choice on his or her own prerogative following a designated confirmation process. For example, a corporation may choose to utilize just a single corporate registrar to manage all their contacts, ensuring a higher level of security, while a blogger may choose to use a Validator with a basic level of security. At some point in the future, the blogger could choose a different Validator and "transfer" management of their Contact ID and its associated contact information to that new Validator.
[20] For example, there would need to be some sort of controlled "transfer policy" and "transfer process" most likely similar to current domain name transfer policies and processes.
[21] Additional implementation procedures are needed here. For example, authenticated changes must be propagated to the authoritative data sources for such data, including all domain names utilizing the affected Contact ID. Depending upon the implementation model, this could include domain registries and registrars that store contact data associated with domain names.
[22] Conceptually this could be done at two levels:

26.	If a Contact Holder requests a uniqueness designation, there should be a mechanism provided for other Validators to be able to compare a requested set of contact data against the Contact Holder's [see further analysis below].
27.	Contact Holders should be able to designate who may utilize their Contact IDs in association with domain name registrations. Potential levels of control include: • **Public** – anyone can designate the Contact ID as a contact for their domain • **Verified** – anyone can request the designation of a Contact ID as a contact for their domain, but the holder of the Contact ID must be contacted for approval prior to publishing the Contact ID as part of a domain registration.[23] • **Restricted** – for the highest security, the Contact ID can only be used by the Contact Holder who must be verified via some authentication mechanism. [24]
28.	A Contact Holder should be able to request that the use of their Contact ID in any domain registration (new or update) be tracked/reported and that they receive notification of such events, along with information about the entity making the request.

Summary of Key Benefits

Adopting a Contact ID management and validation system aims to create a more accurate RDS, as it makes it more difficult for those seeking to insert false data into the RDS. This could potentially reduce the incidence of fraud and identity theft.

Specifically, the benefits of this proposal include:

- Greater data accuracy - across multiple registrations, registrars and registries and over time.

- The full contact data set (i.e. the collective name, address, phone, e-mail) as associated with a Contact ID.
- Physically unique element "blobs" (e.g. individual address, phone, e-mail) that are part of a full contact record. Such "blobs" should represent a unique contact point that would in most cases be only usable to a specific person or entity.
- Some addresses may not be unique enough to qualify on their own, so in such cases, exception processes may be implemented.
- Unique data flag requests should be validated at the highest, "identity" level to gain such status.
- New requests to utilize flagged unique data elements without authorization should be blocked and potentially investigated for fraud.

[23] Implication is that some sort of approval/rejection process be created to facilitate such requests.

[24] Potential implementations methods include

- Restricting use of a Contact Id to a single registrar
- Multi-factor approval process to allow use at multiple registrars
- Implication of this is that some sort of status/usability restriction flag be published/provided to go along with the Contact ID itself.

- Increased ability for individuals to control their data.
- Improved efficiency for managing multiple domain names.
- Cost and efficiency improvements for the entire system-[25] Ability for service providers to seamlessly update contact information without needing access to individual domain accounts for domains they have some responsibility for - appear as a contact.
- Reduce abuse occurring via impersonation in registration data.

c. 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 at the same time offering protections for those registrants seeking to protect and maintain their privacy. The EWG recognizes that there are legitimate reasons for individuals to seek heightened protections of their personal information. In addition, some businesses may seek protection of their information for legitimate purposes, such as when they are preparing to launch a new product line. Accordingly, in its Initial Report, the EWG recommended that the RDS accommodate needs for Privacy by including:

- An Enhanced Protected Registration Service for general personal data protection and adherance to local privacy law; and
- A Maximum Protected Registration Service that offers Secured Protected Credentials Service for At-Risk, Free-Speech uses.

Further work on the problems addressed by these two features, along with additional principles and processes now being considered by the EWG, are detailed below. While exploring the complexities of jurisdictional issues, including where to locate any data repositories for the RDS, a common issue raised during the comment period, the EWG discussed the advisability of addressing an overall privacy policy for ICANN that would help ensure a more consistent approach to privacy issues. This new issue is discussed first, as it would set a floor for the approach to data protection.

[25] Note: the implications of this paradigm shift in accountability from registrant to for Contact ID holder merits further consideration.

Binding Corporate Rules

As a major player in the ecosystem of the Internet, and as the multi-stakeholder group which sets policy for the collection, use and disclosure of personal information related to domain registrations, it is important for ICANN to show corporate responsibility in promoting global compliance with best practices in data protection. It is not enough to merely comply with applicable law, or permit opt-outs for contractees such as Registrars to comply with the applicable law in their jurisdiction. Leadership in the matter of the treatment of personal information related to participation on the Internet is expected, given the dynamic leadership role that ICANN plays in promoting a safe, secure, stable Internet.

This is not an easy task, given the lack of an international, harmonized, generally accepted set of privacy laws. Various jurisdictions and international organizations have sought to remedy this gap over the past four decades: the OECD established the OECD Guidelines for the Protection of Personal Information in 1980, the Council of Europe adopted Convention 108 on the protection of Personal Data in 1981, the European Union passed its first Directive on the Protection of Personal Data in 1995, APEC developed its principles in the late 90s, the Standards Council of Canada adopted the CSA Standard for the Protection of Personal Information as a Quality Standard in 1996, and so on. The core principles of what needs to be done from an operational management perspective have been largely agreed, so in keeping with this concept, the European Union has now agreed on what needs to be found in binding corporate rules for international corporations and entities which hold and transfer personal data.

The EWG is considering recommending that ICANN draft a document that sets out how it complies with such internationally accepted management practices. It would perhaps simplify life for actors resident in jurisdictions under data protection law, such as the 28 jurisdictions within the European Union, if indeed ICANN elected to pursue this and submit them as binding corporate rules, but in any case a clear articulation of expected practice and behaviours is required. This in no way pre-empts the application of

relevant law, it merely harmonizes accepted management practices so as to maximize the likelihood of being in compliance with all data protection law, and it provides clear expectations regarding the protection of personal information to all actors, users, and oversight bodies within the Internet ecosystem. It also provides clarity to miscreants who abuse personal information, enabling further action on the part of those who wish to respond to unlawful or abusive behavior.

A framework for discussion of what forms part of a set of binding corporate rules appears in the attached **Annex C**. Further specifications on binding corporate rules have been developed by the Working Party of Data Protection Authorities of the European Union (the Article 29 Working Party) and can be found on the Europa website at http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm.

2) Shield (Privacy) and Proxy Services

Currently, there are services offered to obscure the identity and/or address of entities using domain names, developed because of the open nature of WHOIS. While there are many variants, and no official definitions, here are two generally used acceptable terms:

- A privacy (shield)[26] service provider offers alternate WHOIS contact information and mail forwarding services while not actually shielding the Registered Name Holder's identity.
- A proxy service provider registers a domain name on a third party's behalf and licenses the domain name's use so that the provider's identity and contact information (and not the licensee's) is published in WHOIS.

Neither today's privacy or proxy services are standardized; providers have no contractual relationship with ICANN, although the 2013 RAA introduces the concept of

[26] The EWG is considering using the term "shield" services because calling these "privacy" services may easily confuse users into mistakenly believing these enhanced services deliver durable privacy protections. Given that "privacy" services are often used by companies who are not entitled to personal data protection, it introduces further confusion to refer to the service as a "privacy" service.

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:[27]

> 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*[28] 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.

[27] 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.
[28] Note: The EWG suggests that ICANN consider whether "any problem" might be overly broad.

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

Administrative Contact: [same for Technical Contact]
   Private, Registration
   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.[29] To address both domain name registrant and stakeholder needs for more uniform and reliable Shield and Proxy Services which enable greater accountability, the EWG is considering recommending the following principles:

Suggested Principles for Enhanced Protected Registration Data:

No.	Principles
1.	**General**
1.1	ICANN should accredit Shield (formerly Privacy) and Proxy service Providers
1.2	The accreditation program should continue the commitments under the 2013 RAA Specification
2.	**Principles for Accredited Shield (formerly Privacy) Services**
2.1	Entities and natural persons may register domain names using accredited Shield services that do not disclose the registrants contact details unless the terms of service are violated
2.2	ICANN should require specific terms to be included in the terms of service, including, requiring the service provider to endeavor to provide notice in cases of expedited takedowns
2.3	Shield services should provide the registrar with accurate and reliable alternate contact details, including a forwarding email address
2.4	Shield services should be obligated to relay emails received by the forwarding email address
3.	**Principles for Accredited Proxy Services**
3.1	It should be possible for entities and natural persons to register domain

[29] See **Annex B** for studies and reports that document deficiencies with WHOIS as well as privacy/proxy services.

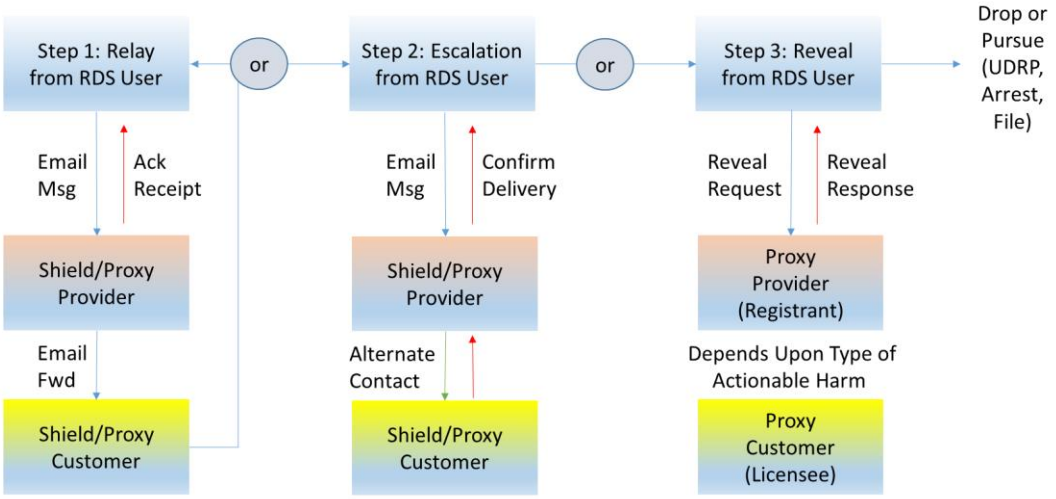
	names using accredited proxy services that register domain names on a licensee's behalf
3.2	Proxy service providers should provide the registrar with their own name and contact details, including a unique forwarding email address
3.3	As the registered name holder, proxy service providers should assume all the usual registrant responsibilities for that domain name, including provision of accurate and reliable registration data
3.4	Proxy services should be obligated to relay emails received by the forwarding email address as further described below
3.5	Proxy services should be obligated to respond to reveal requests in a timely manner as outlined in the escalation procedures below

Suggested Model and Principles for Relay and Reveal

As noted above, the EWG may recommend Shield (privacy) and Proxy Services be required to relay all email received by the forwarding email address. The goal is to provide Shield/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 is considering requiring 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 is now considering a proposal to introduce 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 name (i.e., the Shield Customer or Proxy Provider),
- The admin/tech contact address (including a forwarding email address),
- An indication the domain registration was done via Shield/Proxy Service, and
- Name and address of the Shield or Proxy Service Provider.

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

c) The Shield/Proxy provider should 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 thresholded to deter relay abuse.

d) The RDS user receiving the acknowledgement now has confirmation that the message was relayed to the Shield/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 Shield/Proxy customer to respond and decides to escalate the previously-attempted contact by:

a) Visiting the website of the Shield (privacy) or Proxy Service identified in step 1 and completing an escalation form that contains:

- The RDS user's identity (possibly reusing an RDS query credential)
- The RDS user's reason for contact (could be a pull-down list of defined reasons)
- The Shield/Proxy-registered domain name
- An uploaded message to be relayed to the customer (possibly encrypted?)
- Timestamp of when relay was first attempted

b) The Shield/Proxy Provider should 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*[30] days. Here again, negative confirms would be returned for error cases (e.g., unauthenticated user, timeout) and submissions could be logged and thresholded to deter abuse.

c) The RDS user receiving the confirmation now has documented proof that the message was delivered to the Shield/Proxy customer. Still, the customer may choose not to reply, but escalation should 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 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 Proxy Service identified in step 1 and submitting a reveal request that contains:

[30] * 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.

- 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 # from escalation?)

b) The Proxy Provider should be required to investigate and take appropriate action (see d), returning a "reveal response" within N*[31] days. Reveal requests could be logged, limited to actionable harms, alleged by RDS users with standing,[32] to deter abuse.

c) The 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 should 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 impact of local law and factors to be considered. All of the above happens today, without any oversight or 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 law enforcement criminal investigation might lead to a

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

[32] ** 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.

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 Proxy.

Note that the processes described above do not address when a shielded or privacy registration should be "unmasked" to the public rather than simply "revealed" to the requestor. The EWG is interested in exploring this issue further and updating its proposals once it has examined the results of the research to be conducted (see Section V).

Secured Protected Credentials

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 well 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, and if the details are not available on the Internet, it most certainly means that the pursuers of these individuals or groups will target 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 the proposed secure credentials offering is to provide secure anonymous registration for individuals or groups under threat, who wish to exercise rights of free speech on the Internet which are widely regarded as protected, or where identification of speakers would 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 population at large, 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 needs to publish service times for their members who know the address.

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 the witness protection program. Shelters for women who suffer domestic abuse may need to advertise their services on the Internet, and secure contact points for information as to how to reach the shelter, only for genuine victims. Individuals who have had an identity change, along with their families, 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, and wish to run a website where they can provide details on what is going on in their home country, or the persecution to which they are being subjected. The government in power may pursue the website, alleging treason or other crimes, after documentation of the ruling party's abuse appears 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, but 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

Ethic groups often suffer harassment and discrimination and may wish to run websites where they provide vital information for members of the group. For instance, they may wish to run a website where group 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, yet maintain 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 credentials 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, yet without revealing any personal information about themselves, nor providing any trace-back to the transactions which enabled the attributes. Relying parties have secure cryptographic proof that the entity has the authority they are attesting, without needing to know who they are or how they got that authority. This means that any of the vulnerable parties described above (or their representatives) could go to a trusted authority, prove their situation, provide payment for the desired service, and get a trusted credential. They could then take or send the

trusted credential to a proxy registration service and get a domain name. The registrar would have no information about who they are, beyond the requisite technical contacts, and would therefore legitimately not be able to respond to requests for personal or address information. Obviously, there are concerns about technical compliance and abuse and the mitigations of these risks (discussed below), but the key point is that 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 coming in under false pretenses, and staff cannot be expected to understand what kind of unknown threats people may live under, particularly in cases of identity change.
2. A requestor approaches the proxy registrar alleging some kind of criminal or libelous activity and demands to take the website down. In these situations, the Terms of Service (ToC) procedures being developed for Proxy and Shielding Service Operators should be followed. In some instances, such as criminal activity, expedited takedown 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 be forced to use expedited takedown, depending on the relevant law in the jurisdiction.

Even given these limitations, this service would provide much more security to vulnerable registrants than they currently enjoy, and if the new RDS will require enhanced data accuracy and accountability, then a service such as this is required. The following key functions need to be developed:

1. A process to establish criteria for eligibility for secure credentials, starting with the example users 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 requestors (and, in some cases, their agents) are protected. In any anonymous system, this is one of the key weak points.
3. An entity such as an independent tribunal or board to evaluate 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. Accredited proxy providers that would be willing to accept secure credentials, and the financial systems whereby they would be paid.
5. Policies surrounding expedited takedown procedures and other mitigations of abuse.

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 ICANN consider developing Secure Protected Credentials for limited

use, and ensure entities availing themselves of the service do indeed have legitimate need for this Maximum Privacy Protection.

It is also recognized that once a domain name is registered and the website using that domain name 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 obtaining Secure Protected Credentials, and it may be important to provide information underscoring this risk, but ICANN's responsibility ends with the domain name system itself.

Summary of Key Benefits

As described above, with increasing demands for a responsive, accurate directory, with more discipline in the accreditation and procedures applying to proxy and shield services, it will be important to protect the vulnerable. This system would safeguard those who most need to use the Internet for the purposes of free speech and communication within groups, while providing remedies for abuse. It removes a major security risk and potential liability from Registrars, who would **bear the responsibility for** revealing highly sensitive personal information through social engineering attempts. Finally, it would establish procedures for the enablement of vulnerable and disadvantaged groups to benefit from the many advantages of holding their own domains on the Internet.

d. Analysis of Jurisdictional Concerns and Applicable Law

The EWG is currently exploring various mechanisms for accommodating differing jurisdictional concerns for the provision of registration data directory services. The existence of different data protection, consumer protection, cyber-crime, and privacy regimes arising from local laws presents a challenge requiring further attention and

insight. Some of these challenges stem from the fact that some legal regimes are more mature than others in dealing with online issues. For example, cyber-crime legislation is still evolving. In an effort to better understand the legal framework of these jurisdictional issues, the EWG received a legal memorandum highlighting the complexity of these issues, many of which have been raised during the EWG's consultations on the Initial Report.

These jurisdictional concerns are not unique to the new Registration Directory Services (RDS) proposed by the EWG. With the introduction of 1000+ new gTLDs, the potential of conflicts of law with the requirements of today's WHOIS system are magnified exponentially. Prior to new gTLDs becoming operational, registration data was stored by registries in a few numbers of jurisdictions, mostly in the US, with a handful of other countries affected (UK, Ireland, Spain, Hong Kong, and Switzerland).

With 1000+ registries and dozens of back-end registry operators located around the globe, ICANN will be facing increased scrutiny to find a better solution for addressing these conflicts. Relying on the waiver process under the current WHOIS Conflicts with Privacy Law Procedure is not likely to scale, and could result in inconsistent results for those seeking WHOIS data. While we tend to focus on privacy law, it is important to note that there are many conflicts of law which could apply, notably in areas of consumer protection law.

However, privacy rules continue to evolve and will continue to be the most prominent issue for the foreseeable future. For example, the European Union is developing a new version of the Data Protection Directive 95/46 which could influence the applicability of its rules to the jurisdiction where the registrant is located. The EWG is interested in hearing from the community in Buenos Aires as to how to best address privacy protection and the application of relevant law in the new RDS. The EWG suggests the Binding Corporate Rules as a potential solution, and are interested in reaction to this proposal.

e. Exploration of Possible RDS Models

It was immediately apparent from the feedback received both in person in Durban and from comments received, that the Initial Report had not provided enough detail for the Community to understand the process of analysis undertaken by the EWG in reaching its recommendations. Accordingly, this Status Report provides detail about several alternative models explored by the EWG in preparing its Initial Report, and the EWG continued to test and deepen its analysis of how these might satisfy the recommended principles it had identified. In addition to those models, based on community feedback, additional models were analyzed and compared. All models were evaluated using a set of multi-faceted criteria as identified in **Annex E**.

In conducting its analysis, the EWG articulated the following additional design principles upon which its implementation suggestions are based. These supplement the principles that which were previously identified in the Initial Report, as follows:

Rec.	Design Principles
1.	**Collection:** Today, Registrars or Registrar's Affiliates collect and store registration information from their own customers (registrants). This process is inherently distributed. EWG proposes no change to collection of registration data from registrants by Registrars or Affiliates.
2.	**Storage:** 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, using evaluation criteria reflected in **Annex E.**
3.	**Access:** To protect registrant privacy, a centralized interface should enable appropriate requestor access to registration information across all gTLDs, including anonymous public data access by anyone and authenticated gated data access by accredited users.

4.	**Protocol:** The RDS should use RDAP[33] as the underlying directory access protocol to obtain registration information from storage, wherever that may be.

Additional System Models Considered

In order to test the alternative system models that had been 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 differ in the way that registration information is copied to or queried through the RDS. These differences are summarized in the table below[34] and further explained in **Annex D.**

POSSIBLE MODELS	Collection	Storage	Copy	Access
Current WhoIs	RR	RR/Ry	n/a	RR/Ry
Federated	RR	RR/Ry	n/a	RDS
Aggregated	RR	RR/Ry	RDS	RDS
Regional	RR	RR/Ry	Regional	RDS
Opt-Out	RR	RR/Ry	Optional	RDS
Bypass	RR	RR	RDS	RDS

Comparative Analysis of Aggregated and Federated Models

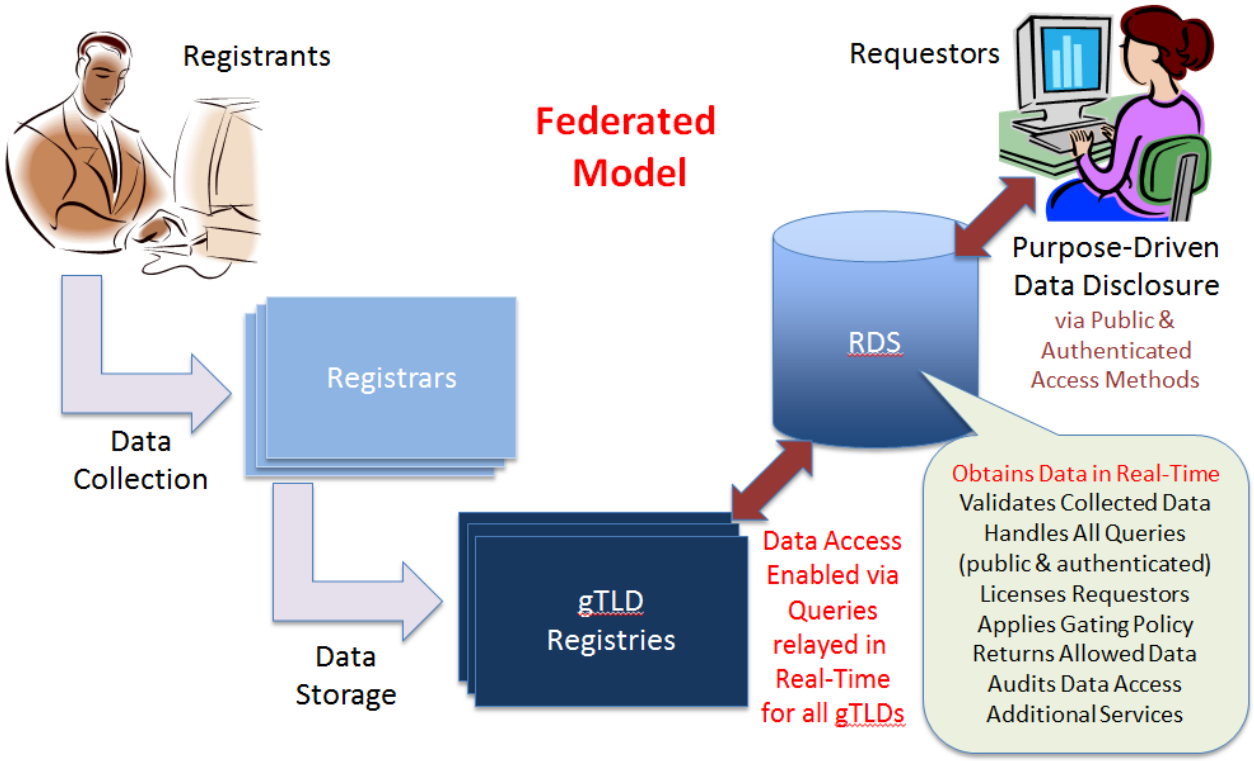
Of the possible system models identified above, each differ in the way that registration information is copied to or queried through the RDS. The EWG closely examined each to determine how these differences might impact different attributes. After comparing these possible models, the EWG found that except for the current Whois, all are capable of satisfying the proposed RDS principles to some degree. Of these, the EWG focused in on the two most promising models for further examination:

- **Federated Model**
- **Aggregated Model (ARDS)**

[33] http://tools.ietf.org/html/draft-ietf-weirds-rdap-query-02
[34] Key for the Table: RR refers to Registrars, RY refers to Registries, RDS refers to Registration Data Service

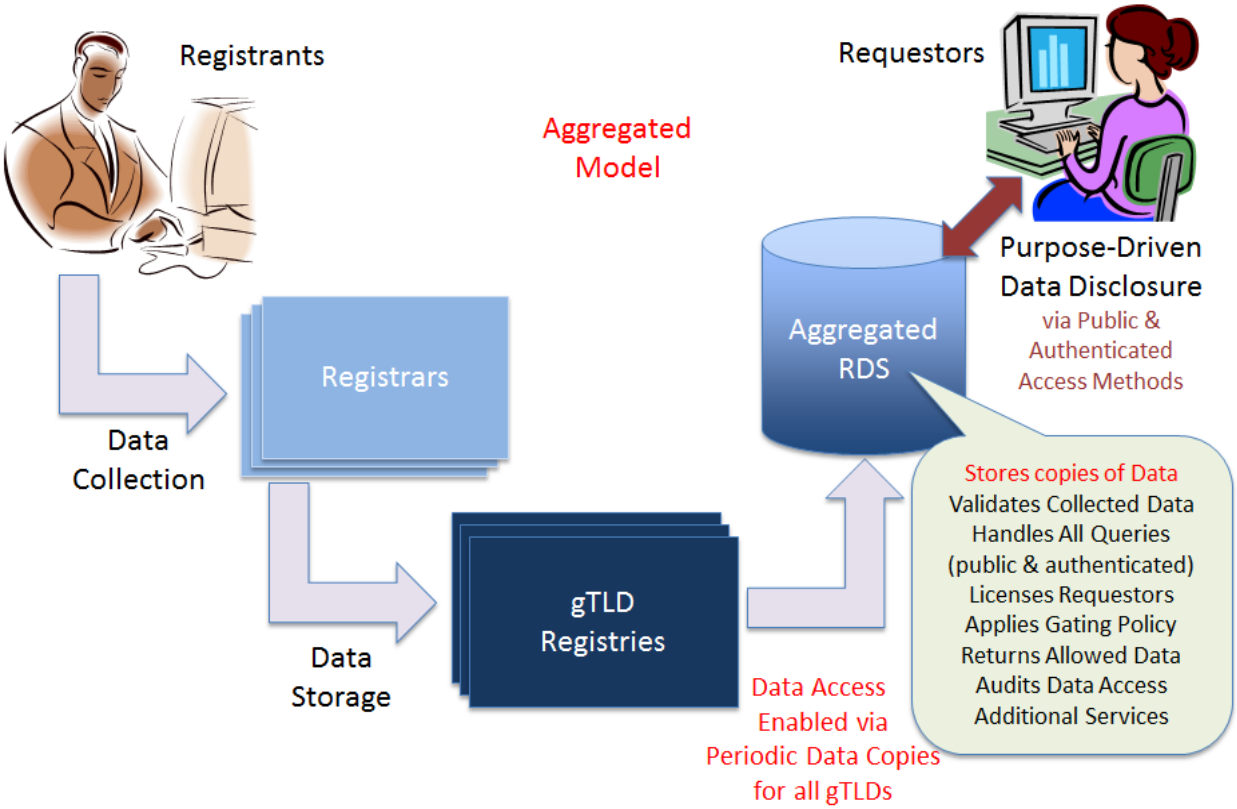
Federated Model

This model describes an RDS that pulls registration information from distributed storage areas, operated by thick Registries, 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.



Aggregated Model (aka ARDS)

This model describes an RDS that periodically copies data from distributed storage areas, operated by thick Registries, into centrally-aggregated storage operated by the RDS. Registries continue to store data, but copies of that data can be used by the RDS to process access requests more effectively.



Described below is a relative comparison of these two EWG-preferred models, after applying the methodology identified in **Annex E.**

- **Security Implications**- Both of these models produce similar result when evaluated against their impact on security. Although there were public comments that an aggregated model such as that suggested in the Initial Report posed a risk due to a "single point of failure," the EWG found that such a risk is not dissimilar from 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 systems and geographically-diversified, redundant infrastructure in order to mitigate these risks.

  An Aggregated Model has the added benefit of being better able to ensure consistent security implementation and policy enforcement. By tightly operating components of the system, an aggregated model managed by one operator would

likely produce a more uniform approach to reaching stated security goals as compared to the Federated Model where potentially thousands of registries and registrars would manage these databases, with differing levels of Registrar/Registry 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 and back-up data centers located throughout the world), whereas the Aggregated Model stores and controls the data in one or more locations, with additional copies retained in other locations (registrar, registry, 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.

  The Aggregated 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 an aggregated RDS) rather than by the potentially thousand+ participants in a Federated Model.

- **Accreditation –** The application of accreditation requirements is possible in both Aggregated 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 an Aggregated Model, as compared with the potentially thousand+ participants in the Federated Model. If a Federated Model were to be adopted, detailed contractual obligations & service level agreements, along with ICANN compliance oversight, would be needed to support consistent enforcement and auditing capabilities.

- **Operation –** The Aggregated 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 an Aggregated Model, where contact data could be translated or transliterated from the contact data 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 an Aggregated 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 an Aggregated Model introduces latency issues that can be overcome by allowing a "real time" lookup at the registry.

- **Implementation –** A Federated Model is more closely aligned to the distributed model of today's Whois, than an Aggregated 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 & registries under the aggregated model by being relieved of the operational burden of constantly responding to complex queries from the RDS interface (such as a reverse Whois) as would be required under a federated system.

f. Support offered by Technical Protocols

Several commentators encouraged the EWG to examine whether the technical protocols deployed in today's domain registration system (such as EPP[35]), 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 proposed model may result in lower transition costs for each of the affected parties.

The EWG analyzed whether EPP could support each data element proposed for inclusion in its proposed RDS, and whether RDAP could support the principles for access credentials proposed by the EWG. The EWG's initial 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 F**.

g. Proposed RDS benefits compared to Current Whois under the 2013 RAA

Several commentators challenged the statement that the Whois is broken. Some believe that the 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, may adequately address the 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 include:

- Anonymous public access of all data elements creates an environment where mining & abuse can occur, with little accountability or ability to remedy
- Limited ability to protect the privacy of individuals

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

- Limited ability to ensure integrity of registration data; registrants can easily insert false contact details, including those held by another
- Lack of Security Features
- Lack of auditing capabilities
- Access not directly linked to stated legitimate purposes
- Inconsistent WHOIS query interfaces and responses
- No support or standards for displaying internationalized registration data
- Limited ability to apply different rules to conform to differing data privacy regimes
- Unacceptable accuracy levels creates inefficiencies for those seeking to communicate with registrants
- Cumbersome management processes to update contacts across multiple domain names
- Difficulties in identifying and communicating with the customers of privacy and proxy services
- No regulation of privacy or proxy services, beyond 2013 RAA requirements that apply only to Registrars and their affiliates

Many of these deficiencies have been documented in the numerous studies conducted over the last decade, as highlighted in **Annex B**.

The EWG is in the process of developing a rigorous comparison of RDS benefits versus the benefits of the current Whois system as improved under the 2013 RAA.

h. Consideration of RDS Costs and Impacts

The EWG also considered RDS costs and impacts. The EWG acknowledges that some aspects of the proposed 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 proposed RDS delivers new and improved services, both benefits and costs must be evaluated. The proposed 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 is unknown today, but includes 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 in today's Whois, such as trademark holders seeking to identify cybersquatters that pay for the services of brand protection companies and commercial Whois services, due in large part to deficiencies in today's WHOIS.

The EWG is evaluating the following cost principles:

Rec.	Cost Principles
1.	Public, anonymous, non-gated access to the data elements should be free
2.	Authenticated, gated access by Law enforcement access to authorized data elements (subject to due process) should be free
3.	RDS design should strive for cost efficiency and minimization, but not necessarily a total reduction in cost
4.	RDS should operate on cost-recovery model; the RDS should not be designed to generate a profit for the operator
5.	A common software platform should be developed and funded by ICANN, to minimized the implement costs on registrars/registries

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 validation fees for pre-validation services).

The RDS may also produce cost savings for registries and who no longer have a requirement 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, or privacy/proxy

service providers). As noted in Section V, the EWG believes a cost/impact analysis of suggested RDS models must be conducted before its recommendations can be finalized.

V. Further Research to Be Conducted

The EWG's future deliberations will include testing and examining the issues and principles identified in Section IV to determine the level of consensus for inclusion in the Final Report. In addition, there are other issues to be explored in detail, such as identifying principles related to compliance and accountability (such as when credentials may be misused, or inappropriate use of data elements accessed through the RDS).

a. Investigation of Applicable Risk/Impact Analysis Frameworks

The Initial Report highlighted the need for a risk and impact analysis to be conducted on various aspects of the proposed model. For example, analysis should be conducted on the risk/impact on registrants incurred by collecting, storing, and disclosing certain data elements through the RDS. This analysis is likely to impact which elements should be made available on a free, public anonymous basis without the presentation of credentials or identification of purpose.

The EWG identified this as a key area for input during the community consultation in Durban. In response, the EWG received numerous comments suggesting a risk/impact analysis be conducted, including a specific recommendation to consider applying the Disclosure Control Framework (DCF), a three phase process that includes risk and utility analysis, application of controls, and assessment. The EWG recommends that a deeper investigation be conducted into the DCF and other potential frameworks that might be appropriate to fully assess the risks and impacts on all stakeholders of the registration data to be collected, stored, and disclosed by the RDS.

b. Inventory of Existing Practices or Shield/Proxy Providers

In an effort to identify appropriate standards for Shield (privacy) and Proxy Providers, the EWG will commence research on the existing practices of current providers of such services, with respect to their relay, reveal, and unmask procedures, and the conditions applicable to them. Also, the EWG is interested in the level of verification or validation conducted by such providers, if any, on the data provided by their customers.

c. Analysis of Data Validation by ccTLD Operators and Commercial Services

Improvements to accuracy levels in the RDS as compared to today's Whois may be achieved through the introduction of increased validation and verification requirements. The requirements that have been imposed by ccTLD providers in their country codes may inform the EWG in determining what levels may be appropriate for generic top level domains, beyond that which has been introduced through the 2013 RAA. For example, the EWG's discussions with Nominet highlighted the novel steps that have been undertaken to reduce inaccurate records. The EWG intends to produce a more thorough catalog of existing ccTLD practices as a reference point as it examines what additional validation or verification methods should apply to the RDS.

In addition, other industries have introduced various levels of validation/verification that may be instructive to the work of the EWG. As a result, the EWG will research the availability of other commercial validation services to determine the difficulty or costliness of recommendations for more robust validation and verification requirements.

d. Identification of Existing Organizations Capable of Accrediting Users

Several commentators questioned the feasibility of creating an accreditation system on a worldwide basis to accommodate the number of uses identified in the Initial Report. For example, meetings with the law enforcement representatives highlighted the difficulties in identifying all types of law enforcement agencies (civil and criminal) that might be eligible for access to the RDS. The EWG will research various user groups

identified in its Initial Report to determine if it is possible to utilize the expertise of existing organizations for this purpose.

e. Cost Analysis of Implementing Possible RDS Models

As described above in Section IV, the EWG is carefully examining the pros and cons of two preferred models, the Aggregated and Federated system models, for its recommended model RDS. Both system models can be designed to satisfy the principles for the RDS proposed by the EWG in its Initial Report. However, if the costs of designing, implementing, and maintaining these models differ significantly, this might lead the EWG to recommend one model over the other. Accordingly, the EWG plans to research the costs associated with each model to inform the next phase of its deliberations.

VI. Next Steps & Timeline for Conclusion

a. Dialogue in Buenos Aires

This Status Report is intended to serve as a discussion document for dialogue with the ICANN community in Buenos Aires on several key issues. Two sessions are scheduled with the ICANN Community on the EWG Work: A public session on Wednesday morning, November 20th providing an overview of the EWG recommendations, followed by an interactive public workshop that afternoon, focused on several key issues where the EWG is seeking specific community input in a roundtable format.

b. Public Input Gathering and Research Nov-Feb

As noted in Section V, the EWG will enter a research phase following the Buenos Aires Meeting to ensure that its recommendations are supported by facts, and are likely to be implementable. During this period, the EWG will suspend its meetings and active work until the results of this research are produced. Further comments from the Community, on this Status Report and any matters raised in Buenos Aires, will be solicited

c. EWG Reconvenes in March

In early 2014, the EWG will reconvene to examine the results of the research conducted and any further comments received, and will finalize its recommendations. The ICANN Singapore Meeting will provide another opportunity to interact with the ICANN Community as the EWG's deliberations conclude.

d. Publication of Final Report

Following the ICANN Singapore Meeting, the EWG will consider the community input received and will produce its Final Report by June 2014. Since the EWG is a Board convened group, its Final Report will be delivered to the ICANN CEO and the Chairman of the Board, for consideration and follow-up. The Board may, for example, forward the EWG Final Report to the GNSO as part of the Board initiated policy development process on the work of the EWG, or, alternatively, may instruct the EWG to conduct further analysis.

ANNEX A: ILLUSTRATIONS OF GATED/PUBLIC ACCESS AND EXAMPLE USE CASE

Example of RDS Registration Data Record

The following registration data record extends the 2013 RAA WHOIS example to reflect proposed 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 choice.

Registration Status: clientDeleteProhibited	Supplied by Registry or Registrar
DNSSEC Delegation: signedDelegation	
Client Status: x	
Server Status: x	
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/	
Domain Name: EXAMPLE.TLD	Collected from Registrant
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 Organization: EXAMPLE ORGANIZATION	
Registrant Company Identifier: D-U-N-S #12345 (issued by Dunn and Bradstreet)	

Registrant Email: EMAIL@EXAMPLE.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 Fax: +1.5555551213 Registrant Fax Ext: 4321 Registrant SMS: +1.5555551213	
Contact Name: EXAMPLE ADMINISTRATOR Contact Role: ADMINISTRATOR Contact ID: xxxx-xxxx Contact Organization: EXAMPLE CONTACT ORGANIZATION Contact Street: 123 EXAMPLE STREET Contact City: ANYTOWN Contact State/Province: AP Contact Postal Code: A1A1A1 Contact Country: AA Contact Phone: +1.5555551212 Contact Phone Ext: 1234 Contact Email: EMAIL@EXAMPLE.TLD Contact Fax: +1.5555551213 Contact Fax Ext: 1234 Contact SMS: +1.5555551213	Registrant may optionally supply Role-based Contact(s)

Key: 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 choice.

PUBLIC ACCESS EXAMPLE: MINIMUM ANONYMOUS QUERY RESPONSE

Returns all public registration data available for queried domain name

Registration Status: clientDeleteProhibited	Supplied by Registry or Registrar
DNSSEC Delegation: signedDelegation	
Client Status: x	
Server Status: x	
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/	
Domain Name: EXAMPLE.TLD	From Registrant
Name Server: NS01.EXAMPLE-REGISTRAR.TLD	
Registrant Type: LEGAL PERSON	
Registrant Contact ID: xxxx-xxxx (issued by RDS-accredited Validator)	
Registrant Email: EMAIL@EXAMPLE.TLD	

Key: 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 choice.

GATED ACCESS EXAMPLE: QUERY RESPONSE TO AUTHENTICATED USER

Returns public and gated registration data available for queried domain name and accessible to identified user, for stated purpose. Here, an authenticated user had permission to query a legal person registrant's name and address, along with all available role-based contacts.

Registration Status: clientDeleteProhibited **DNSSEC Delegation: signedDelegation** **Client Status: x** **Server Status: x** **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 Organization: EXAMPLE ORGANIZATION Registrant Company Identifier: D-U-N-S #12345 (issued by Dunn and Bradstreet) **Registrant Email: EMAIL@EXAMPLE.TLD** Registrant Street: 123 EXAMPLE STREET Registrant City: ANYTOWN Registrant State/Province: AP	Collected from Registrant

Registrant Postal Code: A1A1A1 Registrant Country: AA Registrant Phone: +1.5555551212 Registrant Phone Ext: 1234 Registrant Fax: +1.5555551213 Registrant Fax Ext: 4321 Registrant SMS: +1.5555551213	
Contact Name: EXAMPLE ADMINCONTACT Contact Role: ADMINISTRATOR Contact ID: xxxx-xxxx Contact Organization: EXAMPLE CONTACT ORGANIZATION Contact Street: 123 EXAMPLE STREET Contact City: ANYTOWN Contact State/Province: AP Contact Postal Code: A1A1A1 Contact Country: AA Contact Phone: +1.5555551212 Contact Phone Ext: 1234 Contact Email: EMAIL@EXAMPLE.TLD Contact Fax: +1.5555551213 Contact Fax Ext: 1234 Contact SMS: +1.5555551213	Registrant optionally supplied an Admin Contact
Contact Name: EXAMPLE TECHCONTACT Contact Role: TECHNICAL Contact ID: xxxx-xxxx Contact Organization: EXAMPLE CONTACT ORGANIZATION Contact Street: 123 EXAMPLE STREET Contact City: ANYTOWN Contact State/Province: AP Contact Postal Code: A1A1A1 Contact Country: AA Contact Phone: +1.5555551212 Contact Phone Ext: 1234 Contact Email: EMAIL@EXAMPLE.TLD Contact Fax: +1.5555551213	Registrant optionally supplied a Tech Contact

Contact Fax Ext: 1234 Contact SMS: +1.5555551213	

Key: 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 choice.

Example Use Case Detailing Data Elements

Technical Issue Resolution – Contact with Domain Name Technical Staff

Goal/Scenario
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 (e.g., email sending and delivery issues, DNS resolution issues, web site functional issues.)

Data Elements: The following data elements are relevant for this use case:

Data Collected: A mandatory Registrant Contact ID and optional role-based Contact IDs are collected for each registered gTLD domain name. The Registrant Contact ID may refer to a Natural Person, a Legal Person, or a Proxy Service Provider. A Technical Contact ID may also be available.

Data Requested: For this purpose, the requestor needs data elements enabling real or near-real-time communication with technical staff responsible for a domain name. Requested data may include the Registrant's email address and/or the Technical Contact ID's email address, telephone number, and/or alternative IM/SMS address.

Data Disclosed: Any Requestor may query these data elements, but disclosure depends upon data availability, access policy, requestor identity (if any), and accreditation. For example, anyone can anonymously request and obtain Registrant Email Address. However, authenticated, accredited Technical Users may also query and successfully obtain gated elements available for the domain name and accessible to Technical Users, such as the Registrant's Telephone Number.

Story: A technical person experiencing a problem with a registered domain name tries to obtain contact data associated with that domain by submitting an RDS query, via a web interface or the RDAP protocol.

Three examples are given on the following pages, all returning contact data that may be used to email and perhaps phone someone responsible for resolving technical issues with the affected domain name. Example #1 assumes that legal person registrants are likely to make more data public and so illustrates returning more public data. Example #2 illustrates that minimal personal data is publically available but for specific purposes such as this one, additional gated data may be obtained by authenticated, authorized users. Example #3 illustrates how users might end up emailing or calling a Proxy Provider's Technical Contact for this domain, resulting in a Proxy Provider Relay to the Proxy Customer for this domain.

Example #1: Anonymous query about domain name registered to legal person

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

2) RDS evaluates Query:
No Authentication, because Query is Anonymous
No Authorization, so access to Public Data is Granted
Access is restricted to Public Data needed for Tech Issue Resolution

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

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

Contact ID [12345] and Contact ID [67890] are retrieved from RDS cache or Validator
Obtaining only Public Data Elements for this purpose, including

12345@MerchantZ.gtld Email Address
67890@MerchantZ.gtld Name, Email Address, Phone Number

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

Domain Name: MerchantZ.gtld
Registration Status: clientDeleteProhibited
Client Status: x
Server Status: x
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 Type = Legal Person* *Registrant Organization = MerchantZ, Inc.* *Registrant Contact ID = 12345* *Registrant Email: 12345@MerchantZ.gtld* *<Other Optional Public Registrant Data Elements>*
Contact Name: EXAMPLE TECHNICIAN *Contact Role: TECHNICAL* *Contact ID = 67890* *Contact Email = 67890@MerchantZ.gtld* *Contact Phone Number =+1.1235567890* *<Other Optional Public Contact Data Elements>*

Example #2: Gated query about domain name registered to natural person

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

2) RDS evaluates Query:
   If "A" is Authentic, Gated Query Approved
   If "A" is an Accredited ISP, Access to ISP-Needed Data Elements Granted
   Access is restricted to Public+Gated Data Elements needed by ISPs for Tech Issue Resolution

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

   Registrant Type = Natural Person
   Registrant Contact ID = 12345
   (No Tech Contact ID because Registrant opted not to supply one)

   Contact ID [12345] is retrieved from RDS cache or Validator

Obtaining Public + Gated Data Elements for this purpose, including

12345@PersonY.gtld Name, Email Address, Phone Number

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

Domain Name: PersonY.gtld *Registration Status: clientDeleteProhibited* *Client Status: x* *Server Status: x* *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 Type = Natural Person* *Registrant Name: Example Person* *Registrant Contact ID = 12345* *Registrant Email: 12345@PersonY.gtld* *Registrant Phone: +1.1234512345* *<Other Optional Public Registrant Data Elements>*

Example #3: Gated query about domain name registered to proxy provider

1) User submits Authenticated RDS Query
(DN = ProxyX.gtld, ID=A, Purpose = Tech Issue, Data = All)

2) RDS evaluates Query:
If "A" is Authentic, Gated Query Approved
If "A" is an Accredited ISP, Access to ISP-Needed Data Elements Granted
Access is restricted to Public+Gated Data Elements needed by ISPs for Tech Issue Resolution

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

Registrant Type = Proxy Provider
Registrant Organization = ProxyX, LLC
Registrant Contact ID = 12345
Tech Contact ID = 67890

Contact ID [12345] and Contact ID [67890] are retrieved from RDS cache or Validator
Obtaining Public + Gated Data Elements for this purpose, including

12345@ProxyX.gtld Email Address, Phone Number
67890@ProxyX.gtld Name, Email Address, Phone Number

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

Domain Name: ProxyX.gtld *Registration Status: clientDeleteProhibited* *Client Status: x* *Server Status: x* *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 Type = Proxy Provider* *Registrant Organization: ProxyX, LLC* *Registrant Contact ID = 12345* *Registrant Email: 12345@ProxyX.gtld* *Registrant Phone: +1.1234512345*

Contact Name: EXAMPLE TECHNICIAN
Contact Role: TECHNICAL
Contact ID = 67890
Contact Email = 67890@ProxyX.gtld
Contact Phone Number =+1.1235567890

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 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)
- 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
    - Study on Whois Privacy & Proxy Service Abuse
    - Whois Proxy/Privacy Reveal & Relay Feasibility Survey + Appendices

ANNEX C: FRAMEWORK FOR BINDING CORPORATE RULES

Regardless of the final design, the central theme of RDS is data residency and how operations pertaining to collection, access and transfer are resolved. The major concerns surround data privacy and consumer protection. The strategic response for an adequate global platform is to frame expectations by following the most stringent privacy and consumer protection regulations. The EU privacy provisions could serve as a baseline to address the cross-jurisdictional challenges typically brought to bear in operational processing – collection, access and transfer – of registrant data. Any framework to address the cross-jurisdictional issues must settle on definitions in common and agreeable. Once again, EU privacy law could provide an authoritative definitional baseline for several of the anchor principles. The objectives of the Safe Harbor arrangements are also instructive in this context. While Safe Harbor does not cover not-for-profits and the principles are objectively designed to be less stringent, investigation provides an opportunity to further develop a more elastic framework. Finally and pursuant to the widespread adoption of EU-style data protection laws in non-European jurisdictions and with the provision in EU law for determining 'adequacy' requirements to allow access and transfer of personal data across the EU boundaries, the EWG is evaluating whether to refer and use EU rules as baseline.

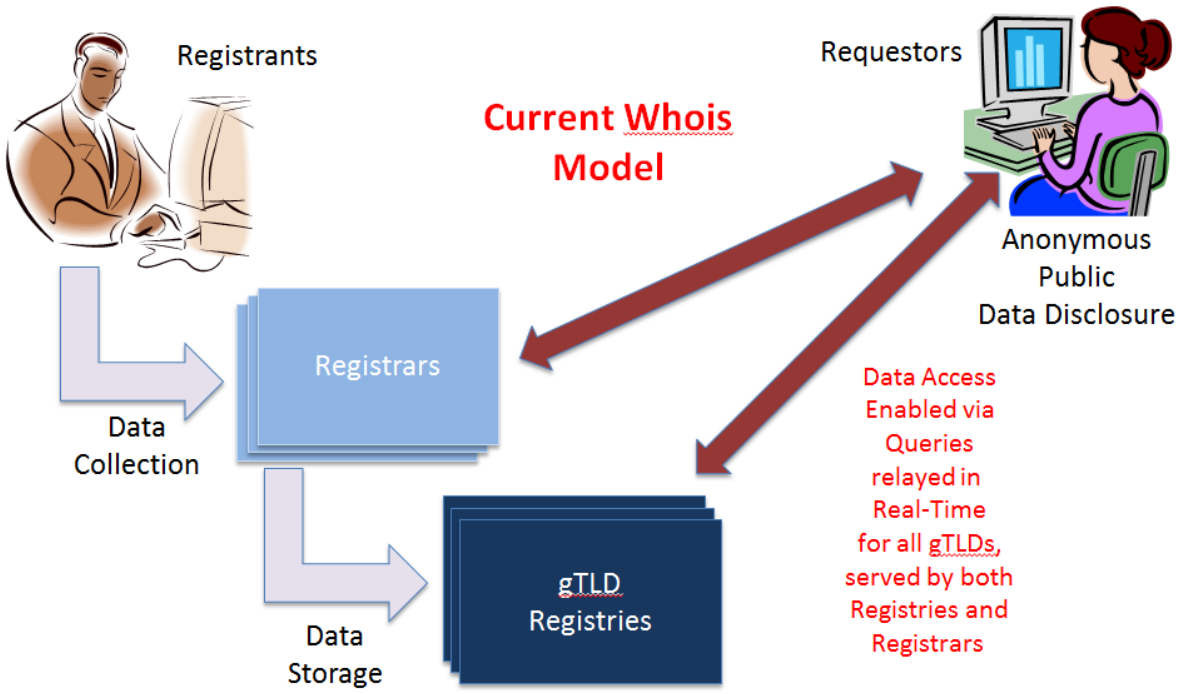
Since ICANN is not a treaty organization, condensation of a set of binding rules that, in principle, commits all participants to obey a set of rules sufficiently mindful of privacy and data protection obligations and which is intended to harmonize processes and practices for all registrant data and which is broadly accepted and implemented is the overall objective. The EWG suggests that these binding corporate rules will provide the right substrate for decisions on collection, processing, accessing and transfer of registrant data.

ANNEX D: DESCRIPTION OF SYSTEM MODELS CONSIDERED

In addition to the models previously described in Section IV.e., the EWG considered the following alternative models but found each of them to be less viable than the Federated or Aggregated Models, for reasons summarized below.

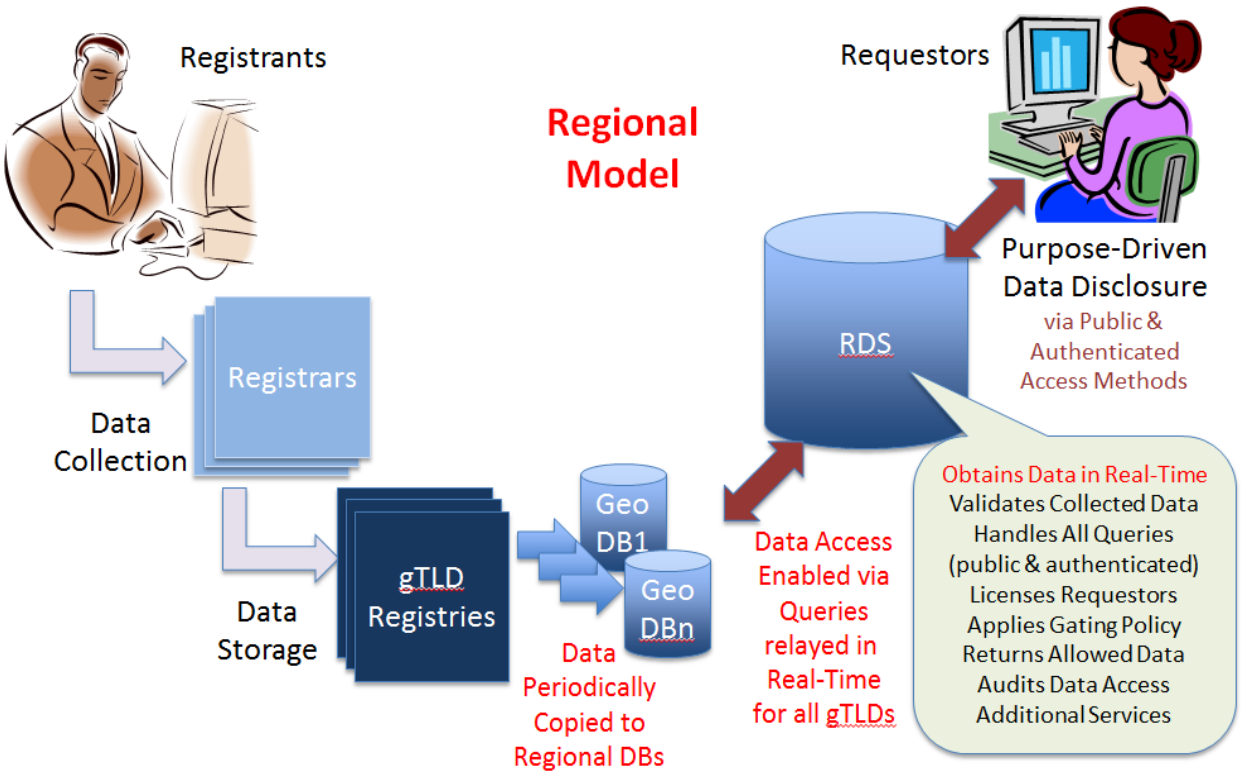
Current Whois

This model describes the fully-distributed autonomous model employed by today's Whois system, with each Registry and Registrar offering its own Whois services without integration across all gTLDs. Although an aggregated 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).



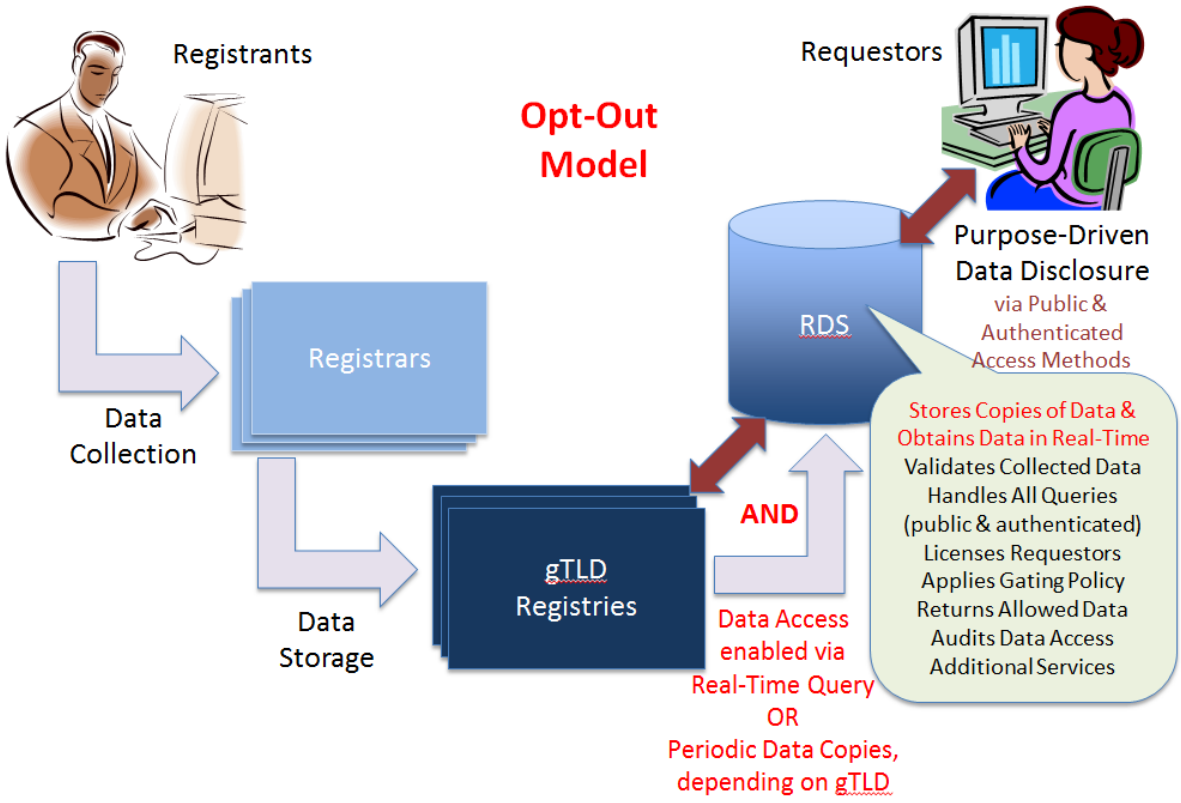
Regional Model

This model describes an RDS that periodically copies data from distributed storage areas, operated by Registries, into regional storage areas located around the world. Registries 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.



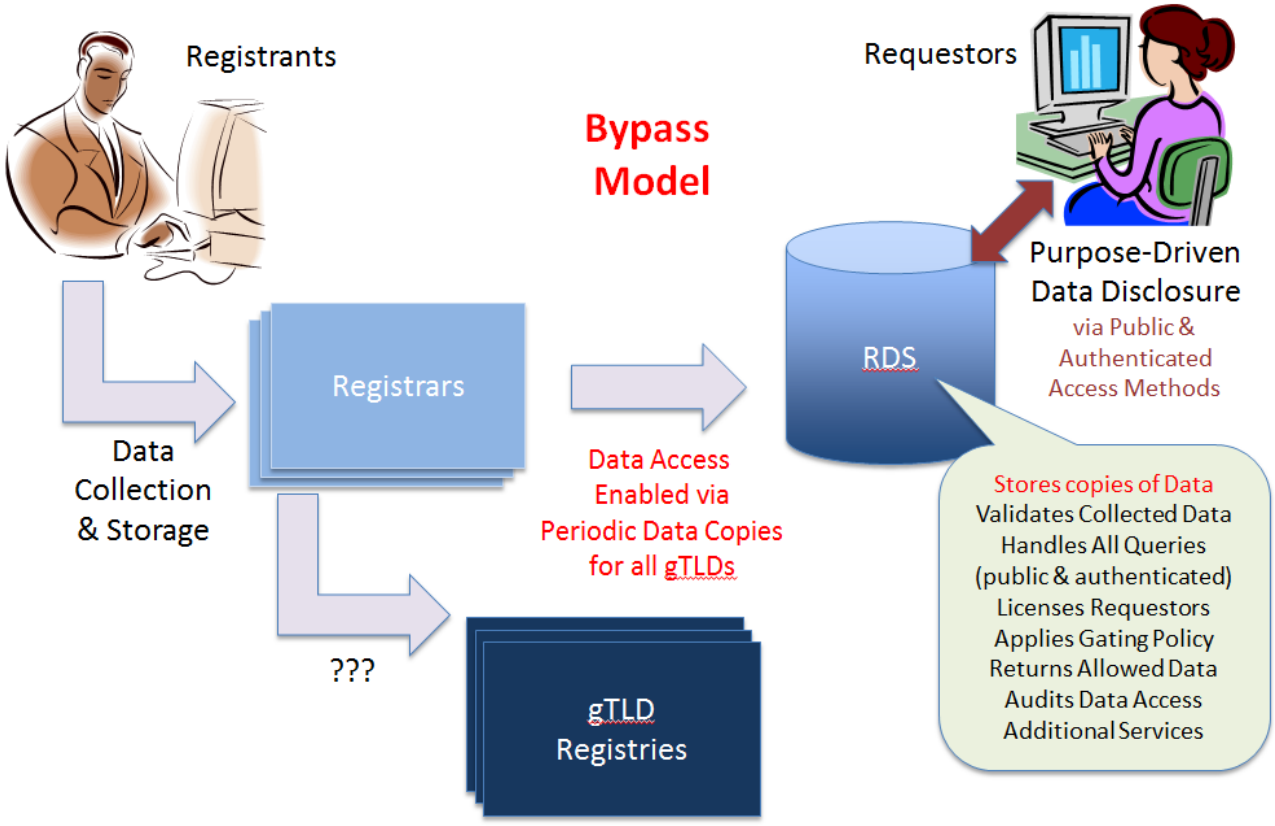
Opt-Out Model

This model describes an RDS that periodically copies data from distributed storage areas, operated by Registries, into centrally-aggregated storage operated by the RDS. Under this model, any Registry can opt out of aggregated storage so long as they agree to provide infrastructure needed to withstand significant querying required to meet availability and performance SLAs.



Bypass Model

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



ANNEX E METHODOLOGY APPLIED TO SYSTEM MODELS

The EWG compared the security pros and cons of each of the possible models against the following criteria:

Security Implications

- **Single Point of Failure:** 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 expertise and investment?

Jurisdiction and Privacy Implications

- **Stores data in local jurisdictions:** Does the model allow for registration information to be stored in one of several jurisdictions? To what extent could Registrants or Registrars 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 registration information to be accessed 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 which 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?
- **Track/Audit/Penalize Requestors:** How effectively and reliably can the model log and audit 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)?

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 update 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) on the speed at which requests can be handled 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/herown 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 role-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 the 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 operating 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 in new/modified infrastructure and processes overall, as compared to other models? Here, a model that with lower cost of implementation overall 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 use cases:

- Domain Name Acquisition
- Domain Name Registration History
- Domain Names for Specified Registrant
- UDRP Proceedings
- Investigate Abusive Domain Name
- Deter Malicious Internet Activities

ANNEX F: ABILITY OF EPP AND RDAP PROTOCOL TO SUPPORT RDS

Data Elements and Accessibility

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
Contact role	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 Expiry Date	Y	Y
Registrant type	N	Y*
Contact Name	Y	Y
Contact ID	Y	Y
Contact Organization	Y	Y
Contact Street Address	Y	Y
Contact City	Y	Y
Contact State/Province	Y	Y
Contact Postal Code	Y	Y
Contact Country	Y	Y
Contact Email Address	Y	Y
Contact phone + Ext	Y	Y
Contact Fax + Ext	Y	Y
Updated Date	Y	Y
Registrant Name	Y	Y
Registrant Contact ID	Y	Y
Registrant Organization	Y	Y
Registrant Company Identifier	Y	Y
Registrant Street Address	Y	Y
Registrant City	Y	Y

Data Element	EPP Support for Collection	RDAP Support for Access
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 Address	Y	Y
Registrant SMS/IM/etc	N	Y
Registrar URL	N	Y
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 SMS/IM/etc: Would need to be added to EPP by protocol extension.

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