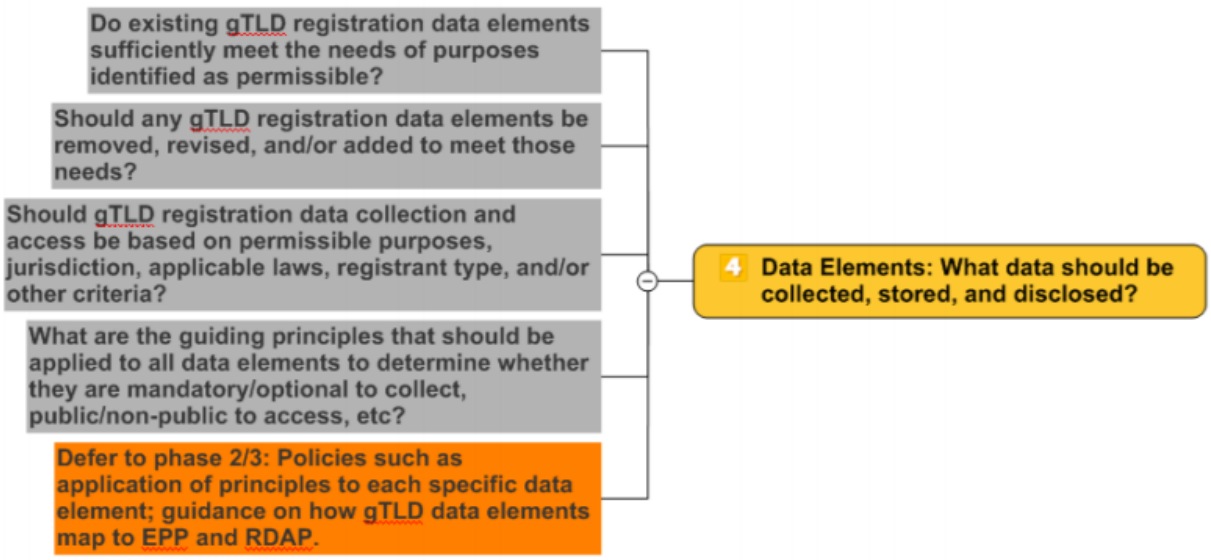
From the RDS PDP WG Charter:



Approach to deliberating on this Data Elements charter question: Concentrate on the superset of data elements that may be collected and possibly displayed in the RDS. That is, review the entire table of proposed elements, decide what to delete/add, then decide what to collect/display.

The following excerpts are taken from the EWG Final Report:
https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf

EWG Report	Description of Contents	Handout
Pages 129-132	Annex D: List of Data Elements and associated Purposes	Slides 2-5
Pages 49-51	Table of Individual Data Elements	Slides 6-8
Pages 47-48	Legend for above Table of Individual Data Elements	Slides 9-10
Pages 57-58	Description of proposed new Data Elements not included in 2013 RAA	Slides 11-12
Pages 36-39	Overview of Purpose-Based Contacts and their Responsibilities	Slides 13-16

Note: Minimum Public Data Set (MPDS) elements have already been discussed, so the 28 June Poll focuses only on data elements beyond the MPDS. Data elements in the MPDS have therefore been greyed out on pages 129-132 to follow.

ANNEX D: PURPOSES AND DATA NEEDS

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

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

MPDS = Grey

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

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

MPDS = Grey

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

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

MPDS = Grey

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

See slides 9-10 for Column Legend

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

See slides 9-10 for Column Legend

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

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

See slides 9-10 for Column Legend

Resulting Data Element Classifications -- Column Legend for Slides 6-8

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

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

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

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

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

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

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

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

[4] For data collected from Registrants,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

f. Purpose-Based Contact Roles and Responsibilities

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

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

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

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

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

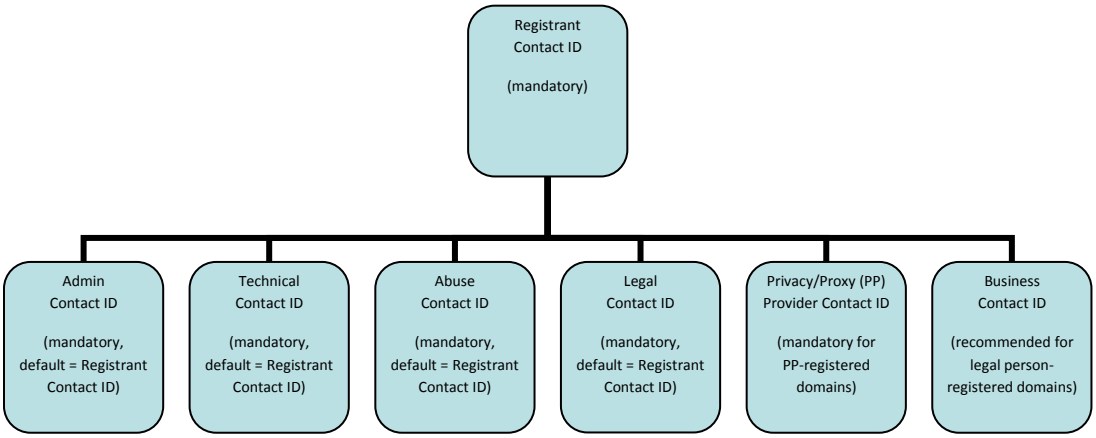


Figure 4. RDS Contact Types

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

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

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

Example DN Record:

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

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

Example DN Record:

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

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

Example DN Record:

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

colors above provide visual correspondence to graphic below

These examples are illustrated graphically in the following figure:

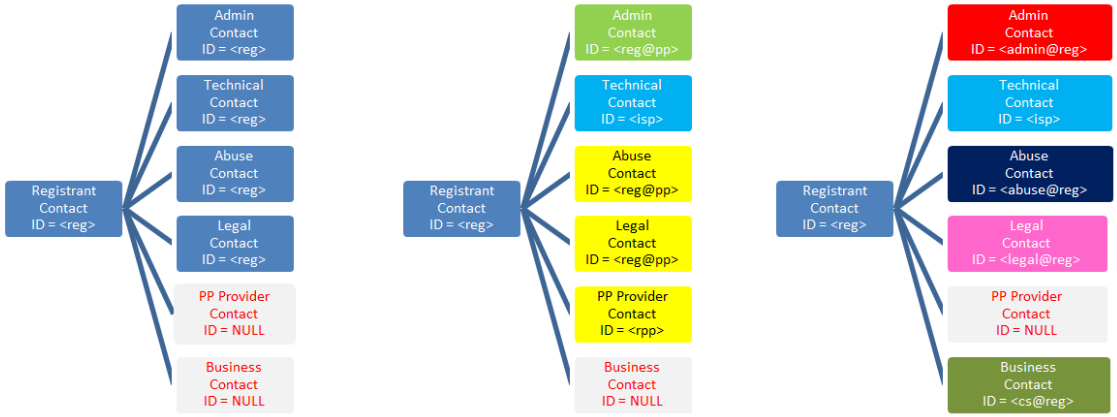


Figure 5. Example DN Registrations using Purpose-Based Contacts

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

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

Potential responsibilities for each PBC can be summarized as follows:

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

Table 5. Potential Responsibilities for each Purpose-Based Contact

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

g. RDS Contact Use Authorization

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