# Subquestion 5.1: *Should gTLD registration "thin data" be entirely public or should access be controlled?*

## Rough Consensus WG Agreement from 2 May WG Call and Poll:

"gTLD registration "thin data" should be accessible without requiring inquirers to identify themselves or state their purpose."

This agreement is limited to "Thin Data" Elements, for example:

Domain Name: ANVILWALRUSDEN.COM
Registrar: TUCOWS DOMAINS INC.
Sponsoring Registrar IANA ID: 69
Whois Server: whois.tucows.com
Referral URL: http://www.tucowsdomains.com
Name Server: NS1.SYSTEMDNS.COM
Name Server: NS2.SYSTEMDNS.COM
Name Server: NS3.SYSTEMDNS.COM
Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Updated Date: 17-jan-2017
Creation Date: 30-jun-2010
Expiration Date: 30-jun-2017

Note: We still need to finish deliberating on Purpose and Data Elements to agree upon required "Thin Data" Elements and their purposes.

# Continue deliberation on Charter Question 5:
# *What steps should be taken to control "thin data" access?*

**Q2:** Building on agreement: ***"gTLD registration "thin data" should be accessible without requiring inquirers to identify themselves or state their purpose,"*** the following alternatives for a possible requirement were suggested during and after last week's WG call. Below are 9 May Poll results indicating levels of support:

| Q2 Response | a) "Thin data" elements should be accessible with or without requestor authentication. | b) "Thin data" elements should not require requestor authentication, but must allow for optional authentication of the requestor. | c) "Thin data" elements are to be accessible, regardless of the level of authentication of the requestor. | d) "Thin data" elements are to be accessible, regardless of the level of authentication, or lack thereof, of the requestor. | e) "Thin data" elements should be accessible without requester authentication. | Total |
|---|---|---|---|---|---|---|
| This is my preference | 10 | 4 | 8 | 7 | 15 | 44 |
| I could live with this | 11 | 10 | 16 | 16 | 9 | 62 |
| I do not support this | 9 | 11 | 4 | 3 | 4 | 31 |
| Total Support - Objections | 11 | 3 | 20 | 20 | 20 | |

https://community.icann.org/download/attachments/64078620/SummaryResults-Poll-from-9MayCall.pdf

# Continue deliberation on Charter Question 5:
# *What steps should be taken to control "thin data" access?*

Using 9 May Poll responses to identify possible requirements for further deliberation:

a) Is "thin data" access authentication required or allowed?

- Proposed answer: Based on Poll Question 2) Option e):
  *"Thin data elements must be accessible without requestor authentication."*

b) Is "thin data" access anonymity required or allowed?

- Proposed answer: Based on Poll Question 2) Comment 9:
  *"Access to thin registration data must be provided to anonymous requestors."*

c) Define "anonymous" and "authentication"

# Definitions that may be helpful

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Note that the force of these words is modified by the requirement level of the document in which they are used.

1. MUST This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

2. MUST NOT This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

3. SHOULD This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

4. SHOULD NOT This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

5. MAY This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item.

Source: https://www.ietf.org/rfc/rfc2119.txt

# Definitions that may be helpful

$ anonymity
(I) The condition of an identity being unknown or concealed. (See: alias, anonymizer, anonymous credential, anonymous login, identity, onion routing, persona certificate. Compare: privacy.)

Tutorial: An application may require security services that maintain anonymity of users or other system entities, perhaps to preserve their privacy or hide them from attack. To hide an entity's real name, an alias may be used; for example, a financial institution may assign account numbers. Parties to transactions can thus remain relatively anonymous, but can also accept the transactions as legitimate. Real names of the parties cannot be easily determined by observers of the transactions, but an authorized third party may be able to map an alias to a real name, such as by presenting the institution with a court order. In other applications, anonymous entities may be completely untraceable.

$ anonymous login
(I) An access control feature (actually, an access control vulnerability) in many Internet hosts that enables users to gain access to general-purpose or public services and resources of a host (such as allowing any user to transfer data using FTP) without having a pre-established, identity-specific account (i.e., user name and password). (See: anonymity.)

Source: https://tools.ietf.org/html/rfc4949

# Definitions that may be helpful

$ authentication

(I) The process of verifying a claim that a system entity or system resource has a certain attribute value. (See: attribute, authenticate, authentication exchange, authentication information, credential, data origin authentication, peer entity authentication, "relationship between data integrity service and authentication services" under "data integrity service", simple authentication, strong authentication, verification, X.509.)

Tutorial: Security services frequently depend on authentication of the identity of users, but authentication may involve any type of attribute that is recognized by a system. A claim may be made by a subject about itself (e.g., at login, a user typically asserts its identity) or a claim may be made on behalf of a subject or object by some other system entity (e.g., a user may claim that a data object originates from a specific source, or that a data object is classified at a specific security level).

An authentication process consists of two basic steps:

- Identification step: Presenting the claimed attribute value (e.g., a user identifier) to the authentication subsystem.
- Verification step: Presenting or generating authentication information (e.g., a value signed with a private key) that acts as evidence to prove the binding between the attribute and that for which it is claimed. (See: verification.)

Source: https://tools.ietf.org/html/rfc4949

# Continue deliberation on Charter Question 5:
# *What steps should be taken to control "thin data" access?*

Using 9 May Poll responses to identify possible requirements for further deliberation:

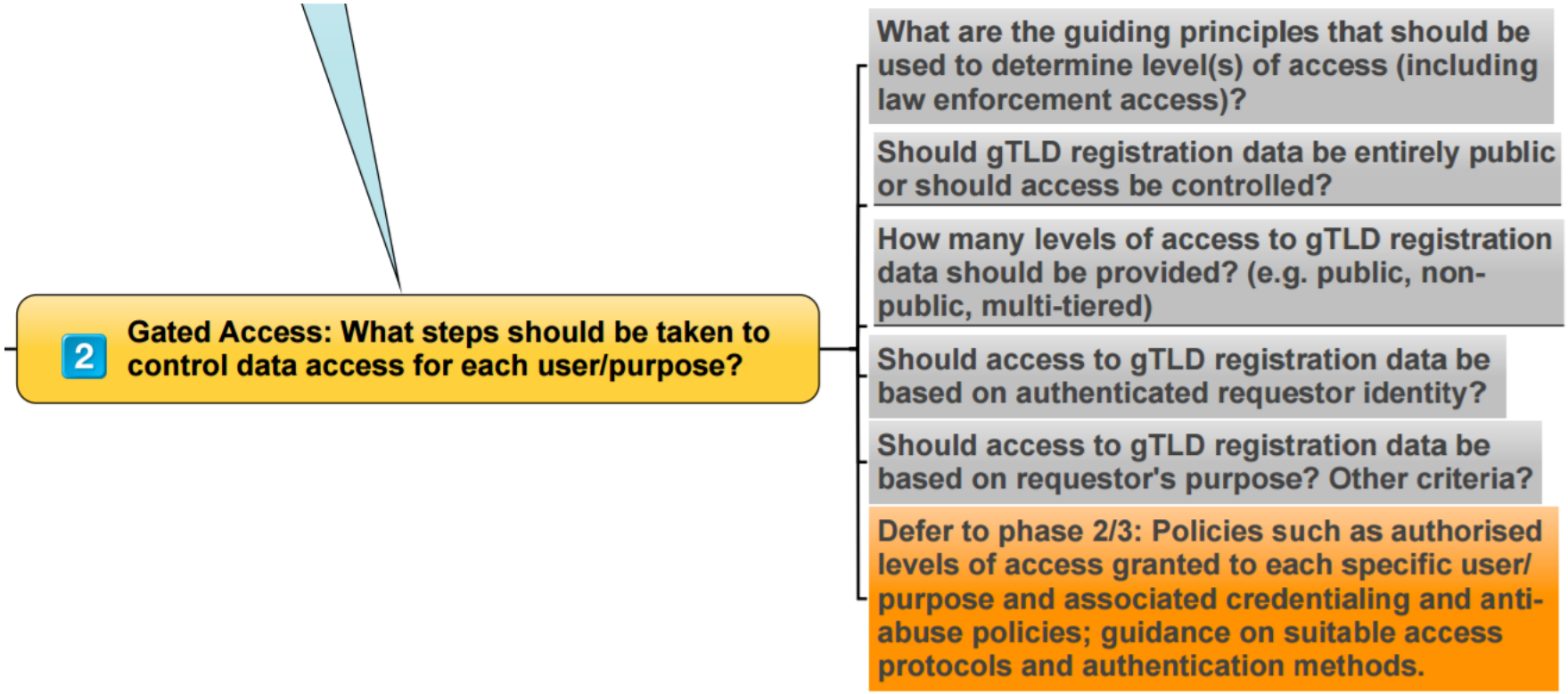
d) Should policies allow or prevent application of operational controls?

- Rough consensus WG Agreement (75%) on Poll Question 3):

  *"There must be no RDS policies that prevent RDS operators from applying operational controls such as rate limiting and CAPTCHA, provided that they do not unreasonably restrict legitimate access."*

- Comments identified need to define specific policies for "reasonable" and "legitimate" – could such policies be defined during Phase 2 of this PDP?

# Returning to Charter Question 5: Gated Access – Plan to complete deliberation?




Source: RDS-PDP-Phase1-FundamentalQs-SubQs-MindMap-2May 2016.pdf

# EXCERPTS FROM INPUT MATERIALS FOR REFERENCE AS-NEEDED

# Related Input Materials

Final Issue Report [PDF] (7 October 2015), especially

- Section 4.2, Gated Access
- Annex C, Charter – Gated Access Question, Phase 1 Goals (Page 70)

EWG Recommendations for a Next-Generation RDS, especially

- Section 4b, Principles for Unauthenticated and Gated Data Access
- Annex E, Unauthenticated and Gated Access Examples
- Video FAQs "Does the RDS eliminate free public access to data?" and "What would I need to do to access gated RDS data?
- EWG Tutorial Pages 15-21, 42-60

Question 5: https://community.icann.org/download/attachments/64078601/ICANN58-DataProtectionExpert-Responses-7April2017-plus-Intro.pdf

https://community.icann.org/display/gTLDRDS/Phase+1+Documents

- KeyConceptsDeliberation-WorkingDraft-21April2017.pdf, Section 5
- All WG decisions are added to this document during deliberation

# Relevant Question/Answer from ICANN58 Data Protection Experts

5. Below is an example of "thin data" elements made publicly accessible in today's WHOIS system for every registered gTLD domain name. Do you believe that any of the following data elements are considered personal information under the General Data Protection Directive, and why?

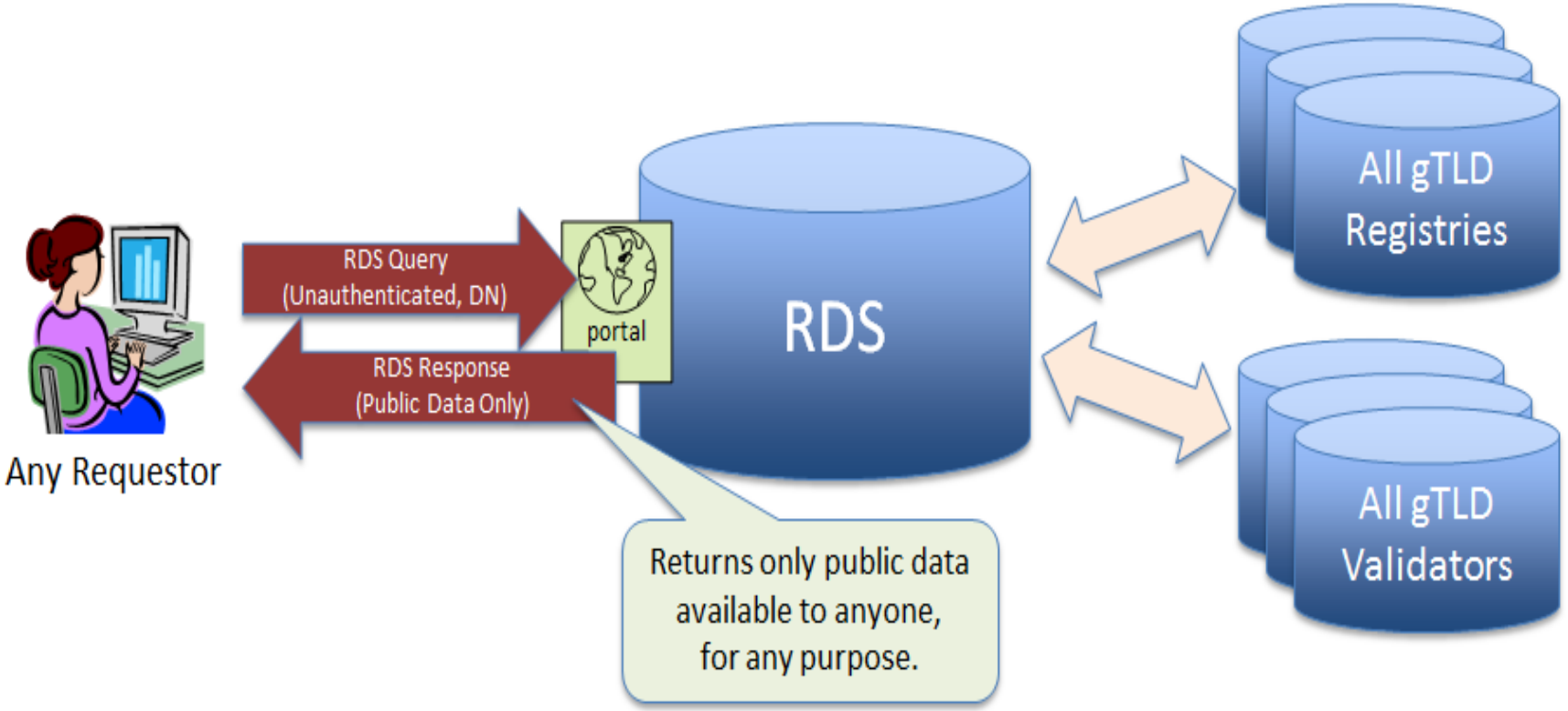
Domain Name: CNN.COM
Registrar: CSC CORPORATE DOMAINS, INC.
Sponsoring Registrar IANA ID: 299
Whois Server: whois.corporatedomains.com
Referral URL: http://www.cscglobal.com/global/web/csc/digital-brand-services.html
Name Server: NS-1086.AWSDNS-07.ORG
Name Server: NS-1630.AWSDNS-11.CO.UK
Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Updated Date: 15-feb-2017
Creation Date: 22-sep-1993
Expiration Date: 21-sep-2018

**This information can be easily combined with other data sets freely or easily accessible, then yes, it is "personal data". Google itself is offering look up services, reverse look up services (for free). Besides there are websites which are harvesting data from whois.corporatedomains.com and making them accessible freely with personal data as on WHOIS Servers there is personal data. (see: www.who.is for instance). As long as the identification of a person behind this information and numbers is possible, it is considered as personal data.**

Source: https://community.icann.org/download/attachments/64078601/ICANN58-DataProtectionExpert-Responses-7April2017-plus-Intro.pdf

Answer to 5.1 given by the EWG Report, Pages 61-62:

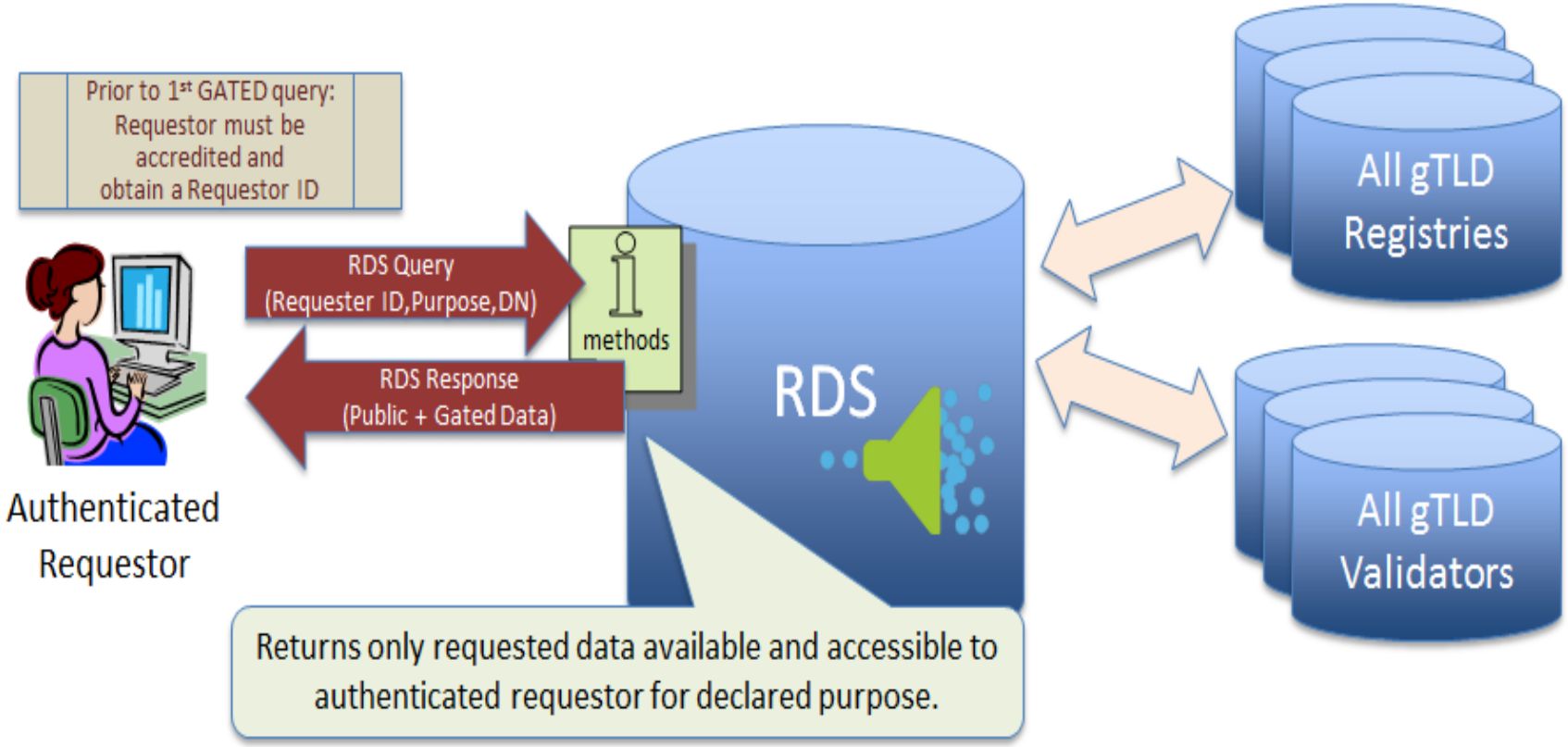
*As depicted in the following figure, public data elements can still be requested from the RDS by anyone, with or without authentication.*




*A minimum set of data elements, at least in line with the most stringent privacy regime, must be accessible by unauthenticated RDS users.*

Answer to 5.1 given by the EWG Report, Pages 61-62:

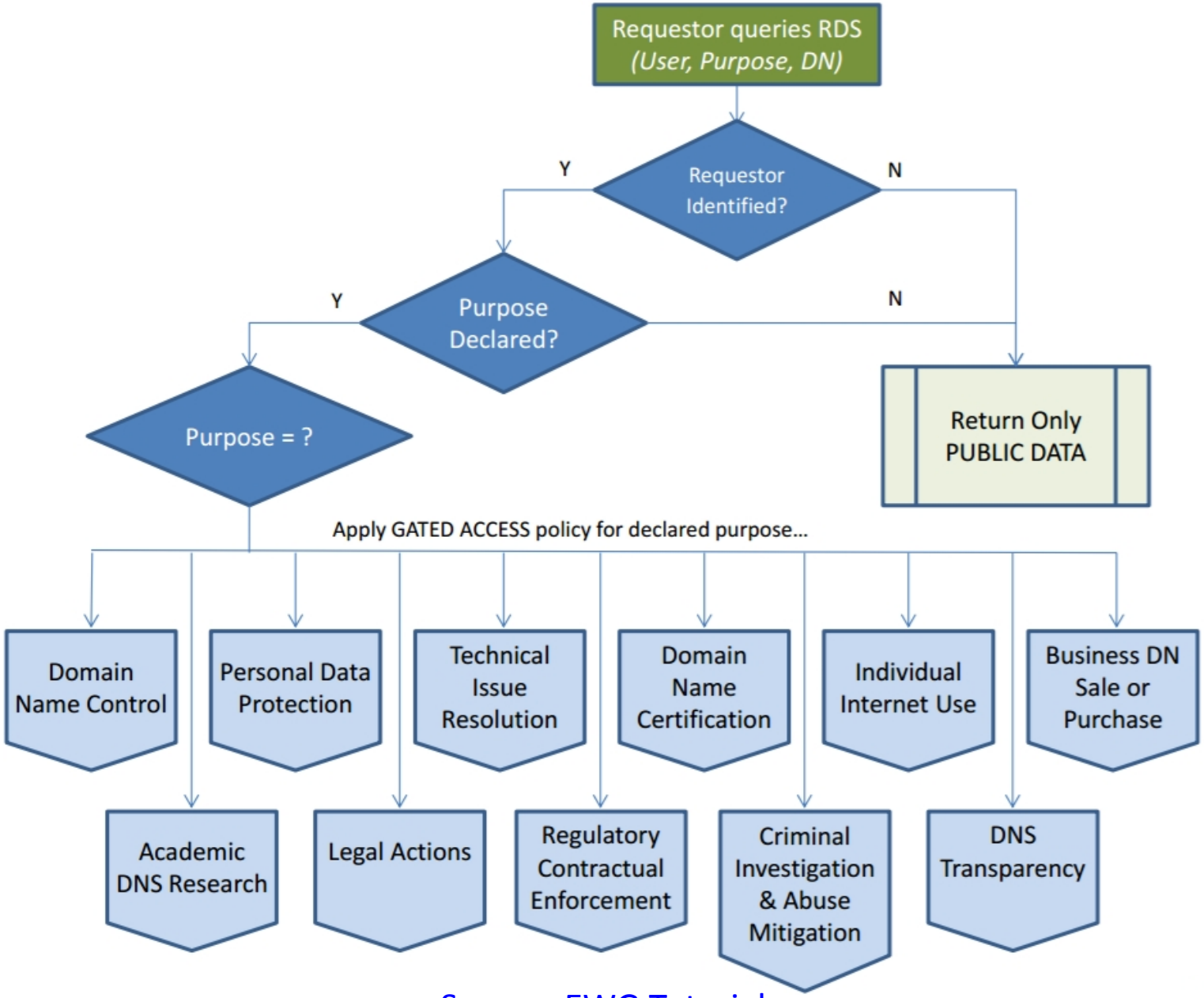
*As depicted in the following figure, gated data elements can also be requested via the RDS. To do so, requestors must first be accredited. Thereafter, requestors may submit authenticated queries requesting data elements for a stated purpose.*




*Multiple levels of authenticated data access must be supported, consistent with stated permissible purposes.*

# How does this differ from WHOIS?

- The EWG Report split RDS Data Elements into categories
  - Minimum Public Data Set (includes today's "thin data" elements)
  - Gated Data (includes most of today's "thick data" elements)
  - See EWG Report for definitions and criteria
- Requestors optionally IDENTIFY and AUTHENTICATE themselves
  - Anonymous RDS queries return ONLY Minimum Public Data Set
  - Authenticated RDS queries may or may not return Gated Data Subset
- Requestors optionally state a PURPOSE
  - Users can be ACCREDITED for one or more purposes
  - Accredited users are AUTHORIZED to access Minimum Public Data Set + Gated Data Subset AS NEEDED BY PURPOSE & LIMITED BY APPLICABLE LAW
- Requestors optionally ACCREDITED for RDS access, for example
  - Self-accreditation for purposes authorized to access to low-risk data
  - Third-party accreditation for purposes with access to higher-risk data
- No identification or authentication? No purpose?
  - Such queries return ONLY Minimum Public Data Set
- Anti-abuse measures such as RATE LIMITING apply to all kinds of RDS access




Source: EWG Tutorial