Building Block i) *(Query Policy – entity disclosing the data)*

Staff support team comment:
Re. of an abuse nature: From use case template, consider including specific examples of what is considered abusive to ensure that no legitimate and/or authenticated requestors are blocked.
Rec b) From use case template: To be reworded (Marc A. and Brian to work on suggested alternative language).

The EPDP Team recommends that the entity disclosing the data:

a) May take measures to limit the number of requests that are submitted by the same requestor if it is clear that the requests are not legitimate and of an abusive nature;
b) Must monitor the system and take appropriate action, such as revoking or limiting access, to protect against abuse or misuse of the system, such as unjustified, high-volume automated queries;
c) [Other]

A response to an SSAD request must not include more non-public data elements than have been requested by the requestor. The response must include the public data elements related to the domain name registration.

An SSAD request meeting the requirements as outlined in these policy recommendations must be received for each domain name registration for which non-public registration is requested to be disclosed. Each such request should be examined on its own merits.

Comments / concerns / questions to be considered in relation to building block i):

- *Consider discussing this section further after the entity disclosing the data is identified.*
- *Consider any person who has breached the terms of service should be denied and prevented from being receipt of any disclosure.*
- *Re. b), how could this be enforced? Consider simplifying and merging a) and b).*
- *Re. second paragraph, consider that response should only include elements requested. Also consider further whether the response shouldn't, must not, could, should, or must include public data elements. Consider whether reference to non-public should be removed.*
- *Check whether there is a potential conflict with policy principle #11.*
- *Consider adding: "'"Each such request should be examined (either manually or programmatically) on its own merits."*
- *Consider whether query policy should include the ability to submit multiple requests if linked to the purpose cited.*

Building Block l) *(Query Policy - SSAD)*

The EPDP Team recommends the SSAD, in whatever form it eventually takes, MUST:

a) Unless otherwise required or permitted, not allow bulk access,[1] wildcard requests, reverse lookups, nor boolean search capabilities.
b) Must only return current data (no data about the domain name registration's history);
c) Must receive a specific request for every individual domain name (no bulk access[2]);
d) Must direct requests at the entity that is determined through this policy process to be responsible for the disclosure of the requested data.

Requests must only refer to current registration data (historical registration data will not be made available via this mechanism).

Comments / concerns / questions to be considered in relation to building block l):

- *Dependent on decision on what SSAD actually is.*
- *Further consider bulk access, wildcard requests, reverse lookups or boolean search capabilities – should these not be allowed in any circumstance, or should these be allowed to accommodate some of the use cases identified?*

[1] As described in section 3.3.6 of the Registrar Accreditation Agreement
[2] As defined in section 3.3.6 of the Registrar Accreditation Agreement.

From SSAD Worksheet:

Query policy

Objective: Establish minimum policy requirements for logging of queries, defining the appropriate controls for when query logs should be made available, and if there should be query limitations for authenticated and unauthenticated users of the SSAD.

- How will access to non-public registration data be limited in order to minimize risks of unauthorized access and use (e.g. by enabling access on the basis of specific queries only as opposed to bulk transfers and/or other restrictions on searches or reverse directory services, including mechanisms to restrict access to fields to what is necessary to achieve the legitimate purpose in question)?
- Should confidentiality of queries be considered, for example by law enforcement?
- How should query limitations be balanced against realistic investigatory cross-referencing needs?

Related mind map questions:

P1-Charter-a
a7) How can RDAP, that is technically capable, allow Registries/Registrars to accept accreditation tokens and purpose for the query? Once accreditation models are developed by the appropriate accreditors and approved by the relevant legal authorities, how can we ensure that RDAP is technically capable and is ready to accept, log and respond to the accredited requestor's token?

Annex to the Temporary Specification:
6 Limitations in terms of query volume envisaged under an accreditation program balanced against realistic investigatory cross-referencing needs.
7 Confidentiality of queries for Registration Data by law enforcement authorities.

Materials to review:

Description	Link	Required because
SSAC 101 - SSAC Advisory Regarding Access to Domain Name Registration Data	https://www.icann.org/en/system/files/files/sac-101-en.pdf	Describes effects of rate-limiting.

Related EPDP Phase 1 Implementation: None.

Tasks:
- Confirm definitions of key terms

- Determine full list of policy questions and deliberate each
- Determine possible solutions or proposed recommendation, if any
- Confirm all charter questions have been addressed and documented