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

The EPDP Team recommends that the entity disclosing the data[[1]](#footnote-1):

1. Must monitor the system and take appropriate action, such as revoking or limiting access, to protect against abuse or misuse of the system;
2. May take measures to limit the number of requests that are submitted by the same requestor if it is demonstrated that the requests are of an abusive\* nature;

[\*“Abusive” use of SSAD may include (but is not limited to) the detection of one or more of the following behaviors/practices:

1. High volume automated submissions of malformed or incomplete requests.

2. High volume automated duplicate requests that were previously fulfilled or denied, except in cases where domain name registration data is likely to have changed during an investigation.

3. Use of false, stolen or counterfeit credentials to access the system.

4. Storing/delaying and sending high volume requests causing SSAD or other parties to fail SLA performance. When investigating abuse based on this specific behavior, the concept of proportionality should be considered.

As with other access policy violations, abusive behavior can result in suspension or termination of access to the SSAD. In the event the entity receiving requests makes a determination to limit the number of requests a requestor can submit, further to point b, the requestor may seek redress via ICANN org if it believes the determination is unjustified. For the avoidance of doubt, if the entity receiving requests receives a high volume of requests from the same requestor, the volume alone must not result in a de facto determination of system abuse.

1. MUST respond only to requests for a specific domain name for which non-public registration data is requested to be disclosed and MUST examine each request on its own merits;

A response to an SSAD request must not include more non-public data elements than have been requested by the requestor. The response to a valid/legitimate request must include the public data elements related to the domain name registration; conversely, the response to an invalid/illegitimate request must not include any elements related to the domain name registration

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

The EPDP Team recommends the SSAD[[2]](#footnote-2), in whatever form it eventually takes, MUST:

1. Unless otherwise required or permitted, must not allow bulk access,[[3]](#footnote-3) wildcard requests, reverse lookups, nor boolean search capabilities.
2. Must be able to receive and process a high volume of legitimate requests;
3. Must only return current data (no data about the domain name registration’s history);
4. Must receive a specific request for every individual domain name (no bulk access[[4]](#footnote-4));
5. 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?*

**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 ofrate-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
1. At the moment, it is assumed that the entity disclosing the data is also the entity receiving requests but should this change, this section will need to be updated accordingly. [↑](#footnote-ref-1)
2. “SSAD” is here defined as a system of data disclosure developed under consensus policy and contractually enforced by ICANN. Development of SSAD does not prevent entities from developing additional data processing agreements outside of the consensus policy process to serve their business or customer interests. [↑](#footnote-ref-2)
3. As described in section 3.3.6 of the Registrar Accreditation Agreement [↑](#footnote-ref-3)
4. As defined in section 3.3.6 of the Registrar Accreditation Agreement. [↑](#footnote-ref-4)