Questions and Assumptions regarding SSAD Cost Estimation

On 22 November 2019, the EPDP phase 2 team requested ICANN org to provide costing estimates for both the development and the ongoing operation of a System for Standardized Access/Disclosure of non-public gTLD registration data.

ICANN org has reviewed the request and the "EPDP phase 2 draft initial report" as of 28 November 2019 available at http://mm.icann.org/pipermail/gnso-epdp-team/attachments/20191128/057523ed/EPDPPhase2DraftInitialReport-28November2019-0001.docx. All the references and the analysis in this document is based on the aforementioned version of the document.

In answering the request referred to above, ICANN org's aim is to help the EPDP Phase 2 Working Group with the general and theoretical purpose of evaluating the potential costs of the various models proposed in the draft initial report referenced above. As such, ICANN org is not stating that it would itself carry out any part of the activities required under the proposed models, nor what its own costs would be if it would take on any role in the operation of such models.

ICANN org is requesting the EPDP phase 2 team to confirm the below assumptions on the request and provide responses to the questions below to help us provide the requested estimation. There are open variables in each of the possible models the EPDP team is considering that would directly and significantly impact the cost for their development and operation. The ICANN org team does not want to preempt the EPDP's policy assumptions or implementation details and thus is asking for your input. The answers to these questions about cost variables will help ICANN org calculate cost for an SSAD and identify where the costs may fluctuate for each of the three identified models in the team's initial report, depending on the team's answers to these questions regarding cost variables.

Assumptions:

1. ICANN org is being asked to estimate the costs of three different models. ICANN org understands these three models as follows:
   1.1. Where one entity is responsible for centralized accreditation, authentication, authorization, and disclosure.
   1.2. Where one entity is responsible for centralized accreditation and authentication, while each contracted party provides authorization and disclosure.
   1.3. Where one entity is responsible for centralized accreditation, authentication, and disclosure, while each contracted party provides authorization (like CZDS).
2. ICANN org is being asked to estimate costs for:
   2.1. Developing technical specifications of the SSAD (including open standards).
   2.2. SSAD system(s) development.
   2.3. SSAD system(s) support/maintenance (including enhancements and bug fixing).

2.4. SSAD operation (e.g., customer support, other human resource operators, system operation).

2.5. SSAD periodic auditing.

2.6. SSAD reporting.

3. For this exercise, ICANN org is not going to:

3.1. Estimate costs for contracted parties' systems development and operation or any other indirect costs.

3.2. Estimate costs for requestors' systems development and operation or any other indirect costs.

3.3. Include in the estimates anything related to potential fees (including cost of billing operations) for requestors. This should be addressed at a later stage.

3.4. Include risk mitigation costs, which are variable depending on what role ICANN org is slated to play in the chosen model.

4. As described in recommendation #1(a), the SSAD will only support requestors who are accredited. In other words, a potential requestor will have to be accredited before they can submit a request in the system.

5. The SSAD will be required to support requestors from anywhere in the world. In other words, a potential requestor should be accreditable independently of where they are based.

Questions on Variables Needed for Cost Estimates:

Scaling questions

1. What is the peak load (i.e., number of queries per unit of time) that the system should be designed to support? For reference, during ICANN 63 Nominet shared that they received 800 disclosure requests in a three-month period for a 12 million domain registry. If we were to extrapolate those numbers to gTLDs, the SSAD would handle close to 4,600 requests per month. Alternatively, during the period of October 2018 to September 2019 (latest 12-month period available at time of writing), the total number of Whois queries reported by all gTLDs combined is an average of 244 billion per month. If we only consider searchable-Whois queries, the monthly average for the same period comes to 1.79 million for all gTLDs.

2. How many requestor accounts must the system support?

3. How many accreditations per month should be supported?

4. What service level requirements should be in place for the SSAD for each type of request (e.g., normal, urgent) and sub-elements of the response (e.g., certification, acknowledgement of the request, authentication, authorization, response from the contracted party, actual response to the requestor)?

5. What level of queries by an accredited user or entity should be considered a "threat to the SSAD" such that would trigger rate limiting the requests from such user or entity as described in preliminary recommendation #1(r)?

6. What retention policy for logs should be considered for the cost estimate exercise?

7. What type of assistance and support is to be provided by the identity provider(s) and other actors?

    a. Email support, phone support?

    b. In what language(s) must support be provided?

<u>Periodicity questions</u>

8. With what frequency must the accreditation authority be audited?
9. With what frequency must the identity providers be audited?
10. With what frequency must the entity(ies) disclosing the data be audited?
11. With what frequency must accredited entities/individuals be audited?
12. With what periodicity should accreditations be renewed?
13. What is the definition of a "business day" with regard to an SSAD request? Is that the business day of the requestor, the authorizer, the entity disclosing the data, the gateway operator, other?
14. While the time frame and criteria for urgent requests are not yet established, the placeholder refers to "less than X business days". Is it contemplated that the acceptable range will still be at least one business day?

<u>Design and process questions</u>

15. Is the central gateway required to monitor response time from contracted parties' systems and provide metrics either to ICANN or publicly?
16. Should the SSAD offer RDAP, Web, or both interfaces? Given possible recommendations from the team like the ability to amend or re-submit a request, perhaps RDAP would not be an alternative. However, if there is no RDAP interface, automated processing of responses on the requestor side may not be possible.
17. Should the SSAD be designed to automate authorization of requests, perform manual review, or both?
18. Preliminary recommendation #1(j) notes that the Accreditation Authority "MUST define a dispute resolution and complaints process." Can the team clarify the scope of disputes and complaints that may be contemplated here? Would this include disputes or complaints related to accredited user revocation and abuse, de-authorization of identity providers as described in preliminary recommendation #1? Are there other disputes or complaints envisioned to be included?
19. Is a challenge mechanism contemplated in the event a requestor believes the identity provider improperly rejected their request?
20. What "jurisdictional legal frameworks" of the requestor should be considered as described in preliminary recommendation #7, section 7?
21. Preliminary recommendation #9(f) indicates that the entity disclosing the data "must disclose to the Registered Name Holder (data subject), on reasonable request, confirmation of the processing of personal data relating to them". How would that work for entities that do not have access to contact data for the data subject (e.g., ICANN org, a vendor for ICANN org, the registry, the registrar when the registration has a privacy service not provided by the registrar itself)?
22. Preliminary recommendation #10 says that "unless otherwise required or permitted" search capabilities are not to be offered. It is unclear what the qualification means, i.e., should we consider search capabilities in the cost estimate exercise?
23. Against what standard(s) will the identity provider(s) need to accredit requestors?
24. What version of the EPDP phase 2 report should be used for cost estimation?