9 September 2021

Subject: SSAC2021-09: SSAC Minority Statement EPDP Phase 2A
To: Keith Drazek, EPDP PHASE 2A Chair
From: Rod Rasmussen, SSAC Chair

Dear Keith,

We hereby forward to you for your consideration the SSAC's minority statement for inclusion in the Final Report of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team – PHASE 2A.

The SSAC's minority statement includes the entire body of the SSAC's most recent comment, SAC118, on the EPDP PHASE 2A Initial Report. While we note that the EPDP PHASE 2A team did incorporate some feedback from SAC118 into the Final Report, the substance of SAC118 has not been adopted. The SSAC reaffirms its comments and recommendations from SAC118 as its minority statement.

Our differences aside, the SSAC would like to acknowledge the significant time and effort devoted by the members of the EPDP team and thank them for their contribution on this important topic.

Rod Rasmussen
Chair, ICANN Security and Stability Advisory Committee

SSAC Minority Statement On the Temporary Specifications for gTLD Registration Data - Phase 2A Expediated Policy Development Process Final Report[1]

1 Introduction

The ICANN Security and Stability Advisory Committee (SSAC) appreciates the circulation of the Initial Report of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team – PHASE 2A (hereinafter referred to as "the EPDP 2A Initial Report"),[2] and we thank the working group for the opportunity to comment on it.

In this document the SSAC presents both general comments about the overall Expedited Policy Development Process and specific comments on individual recommendations in the EPDP 2A Initial Report. The SSAC would be happy to discuss these comments with the EPDP team at their convenience to explain any items that may be unclear and require further elaboration.

The SSAC would like to acknowledge the significant time and effort devoted by the members of the EPDP team and thank them for their contribution on this important topic.

2 Background

In this section we review the questions under consideration by the EPDP Phase 2A Working Group (WG), we make some observations about the overall Expedited Policy Development Process, and then we describe our approach. In the following section we present our recommendations, some of which apply to the overall effort and some of which are specific to the Phase 2A effort.

2.1 Questions Under Considerations by the EPDP Phase 2A WG

2.1.1 Distinguishing Natural versus Legal Persons

The General Data Protection Regulation (GDPR) provides specific protection for natural persons (i.e., humans), and no protection for legal persons (i.e., businesses).[3,4] The EPDP WG, and particularly the EPDP Phase 2A WG, has focused considerable attention on this distinction. Among the questions the EPDP WG has considered are:

---

[1] The document was published as SAC118, available at: https://www.icann.org/en/system/files/files/sac-118-en.pdf

[2] See Initial Report of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team – PHASE 2A, https://www.icann.org/en/system/files/files/epdp-phase-2a-initial-report-02jun21-en.pdf

[3] See GDPR Recital 14: "The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person." https://gdpr-info.eu/recitals/no-14/

[4] See GDPR Article 4, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1374-1-1

1. Should there be a specific data element to record whether the registrant is a natural person versus a legal person?
2. Should every registrar be required to make this determination for every registration?
3. What evidence should be required to make this determination?
4. What are the risks if the registrar's determination is incorrect?
5. Should the registrant be required to declare whether they are a natural person or legal person and should the registrar rely on that attestation?
6. Should the contact data for registrants classified as legal persons always be available publicly?[5]
7. Should the contact data for registrants classified as natural persons never be publicly available?
8. Should the status of the registrant be available publicly?
9. How to proceed when the personally identifiable information (PII) of a natural person is included as part of the registration of a legal person?

2.1.2 Feasibility of Unique Contacts

The EPDP team was asked to consider the questions:

- Whether or not a unique contact in the form of a uniform anonymized email address is feasible, and if feasible, whether it should be a requirement?
- If feasible, but not a requirement, what guidance, if any, can be provided to ICANN Contracted Parties who may want to implement uniform anonymized email addresses?

The EPDP team observed that "unique contacts" is a vague term, and that there are two distinct goals stated by those advocating for unique contacts. These are: (1) the ability to quickly and effectively contact the registrant without disclosing personal data, and (2) A common identifier that helps investigators to correlate domain registrations with a common contact.

The EPDP team tried to disambiguate these purposes by proposing two terms:

- **Registrant-based email contact** - an email for all domains registered by a unique registrant [sponsored by a given registrar] OR [across registrars], which is intended to be pseudonymous data when processed by non-Contracted Parties.
- **Registration-based email contact** - a separate single use email for each domain name registered by a unique registrant, which is intended to be anonymous data when processed by non-Contracted Parties.

After some deliberation, the EPDP team did not provide a conclusive answer on the feasibility of registrant or registration-based email contact. The EPDP team recommended that "Contracted Parties who choose to publish a registrant- or registration-based email address in the publicly accessible registration data directory service (RDDS) should ensure appropriate safeguards for the data subject in line with relevant guidance on anonymization techniques provided by their data protection authorities and the appended legal guidance."

---

[5] The EPDP WG generally treats the request and response process as if the "public" data is published for anyone to see. In all anticipated scenarios, all access to registration data is via a request-response process. That is, the registration data is not published in the sense that publication is generally understood. In this document, we use the phrasing "available publicly" to mean data that is available to anyone who requests it without restrictions on use and without attribution.

The SSAC notes that some registrars have already deployed a few different methods to support registrant-based email contact. For example, registrant-based email addresses have been uniquely created for each registrant, hosted with a domain of the registrar. Messages directed to these email addresses are redirected upon receipt by the registrar to the actual recipient. Some registrars provide a web-based form that can be used to direct a message to the registrant of a particular domain name. In most cases, the sender of the original message does not know if the forwarded message was delivered or opened. The Temporary Specification does not provide any service level requirements for the email forwarding.[6,7]

The SSAC is not currently aware of any deployed solution that satisfies the requirements of registration-based email contact as defined above. Anecdotally, a small number of solutions have been proposed but none have achieved any consensus.

2.2 SSAC Observations

Based on participation in the EPDP, SSAC offers two comments regarding the overall effort to achieve a differentiated access system that meets multiple objectives. By differentiated access system, the SSAC means a system that provides the capability for the response to be conditioned based on the requester and the purpose of the request. The System for Standardized Access/Disclosure (SSAD) is a specific example of such a system.

2.2.1 Competing Interests

From the SSAC's perspective, there are three competing interests at work in the policy deliberations.

1. **Privacy advocates.** Some parties want to ensure the contact data for natural persons is not available publicly unless the natural person provides explicit and informed consent to allow public availability. They want this protection to apply to legal persons as well if the contact data includes PII or if PII can be inferred from the contact data.
2. **Data requesters.** Requesters want the maximum amount of data they can get. Requestors want the privacy protections to be as close as possible to only what's legally required. They want requests to be fulfilled reliably, quickly, and inexpensively.
3. **Data controllers.**[8] Those who collect and make the data publicly available, namely registrars and registry operators, want to minimize cost and risk.

Specific individuals or organizations may embody more than one of these competing interests.

2.2.2 An Unspoken Concern

The SSAD is a new system proposed to centrally handle requests for non-public registration data, envisioned in Recommendations 1-18 of the Final Report of the GNSO Expedited Policy

---

[6] Temporary Specification for gTLD Registration Data; Appendix A: Registration Data Directory Services, paragraph 2. https://www.icann.org/resources/pages/gtld-registration-data-specs-en

[7] There have been documented problems with the contactability implementations at registrars. See pp 55-59 of "Domain Name Registration Data at the Crossroads: The State of Data Protection, Compliance, and Contactability at ICANN." http://www.interisle.net/domainregistrationdata.html

[8] The term also includes others collecting or processing the data collected during registration (i.e., resellers).

Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Phase 2.[9]

A well-designed access system will allow requesters with legitimate needs to gain access to non-public data, and to do so reliably, quickly, and inexpensively.

At this time, it is uncertain if we can achieve a satisfactory differentiated access control system. Currently, the ICANN Board has requested a six-month Operational Design Phase (ODP) Assessment to inform its deliberations of the policy recommendations. The proposed SSAD does not yet have a scheduled date of delivery. The initial cost estimate has been criticized by the community as too expensive. There is also a lack of definition as to what data will be available to which requesters, and under what circumstances. Finally, Contracted Parties may be performing manual reviews of data requests, because the EPDP was unable to agree on automation cases.

Due to the lack of clarity on SSAD, some of the participants in the EPDP appear to be assuming the only data they are likely to access for the foreseeable future is publicly available data, and they are pressing to keep the privacy protection to the minimum required by law. The result is an inability to resolve many questions in the EPDP.

2.3 SSAC's Approach

The SSAC believes it is very important for security investigators to get access to domain name registration data. At the same time, it is also important for those who deserve protection to have it. These two alternatives can coexist. But they cannot coexist in the context of a head-to-head argument about whether every single contact should be public or not as the only choice to be made.

It should be possible for contact information which is considered personal, to be held privately and made available under appropriate circumstances to the people who need it. From the SSAC perspective, a timely, reliable, effective, and efficient differentiated access system would make it possible to achieve a result that would be an improvement for all of the competing interests.

Thus, the SSAC believes the focus of the ICANN Community and ICANN org's attention should be to build and operate an effective SSAD.

As things stand, discussion of access to non-public data is outside the scope of the Phase 2A EPDP, and discussion of the Phase 1 and Phase 2 reports is considered closed. Therefore, in this report, we make two kinds of recommendations.

1. Overarching recommendations on differentiated access and the SSAD.
2. Within the scope of the EPDP Phase 2A, we offer some detailed recommendations that, if adopted, make the best of an imperfect situation.

[9] See Final Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process, https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf

3 Recommendations

3.1 Recommendation to GNSO and ICANN org

Recommendation 1: The SSAC recommends the Generic Name Supporting Organization (GNSO) and ICANN org focus their attention on building and operating an effective differentiated access system.

A differentiated access system with the following properties is needed:

Timely	It must come into operation soon.
Reliable	It must operate in a predictable and consistent fashion, both in the operation of the system and the decision-making by the participants of the system.
Useful	It must provide results that are of benefit to the requesters.
Efficient	It must provide responses to legitimate data requests quickly, and at a cost to all the parties that are acceptable for the purpose.
Easily Accessed	Gaining and maintaining credentials has to work well enough to facilitate—rather than impede—use.

This document uses the term "effective" to refer to a differentiated access system fulfilling all the above requirements, and, of course including the functionality required to manage distinct requests and responses to various combinations of requesters and purposes as noted in Section 2.2.

3.2 Recommendations to the Phase 2A EPDP

3.2.1 Legal Versus Natural

From a security practitioner's perspective, the maximum amount of registration data needs to be available for investigation, either through an effective differentiated access system, or through making it available in the public RDDS.

Recommendation 2: The SSAC recommends the following regarding legal versus natural persons:

A. A data element should be defined that denotes the legal status of the registrant. Initially we propose three admissible values: Natural, Legal, and Unspecified. "Unspecified" would be the default value until the registrant identifies themselves as a natural or legal person. This field should be able to support status values depending upon future policy decisions.
B. This data element should be displayed as part of the publicly available data.
C. Registrants should be classified as either natural or legal persons. This should be required at the time of registration, for all new domain registrations. For existing registrations, the value can remain "Unspecified" until it is filled at a later time. Registrars should be required to ask at relevant times, such as upon domain renewal and/or the annual accuracy inquiry, whether the registrant is natural or legal, with the goal of eventually

obtaining that data for all registrants, and reducing "Unspecified" to the lowest practical level.

D. Registrants currently are able to and should continue to have the option of making their contact data publicly available. Legal person registrants should also have the ability to protect their data via privacy and proxy services.

These recommendations are consistent with SSAC's previous advice.[10]

3.2.2 Feasibility of Pseudonymous Email Contact

Recommendation 3: The SSAC recommends the following regarding the feasibility of pseudonymous email contact:

A. The two policy objectives--namely (1) the ability to quickly and effectively contact the registrant without disclosing personal data, and (2) A common identifier that helps investigators to correlate registrations with common contacts should be considered separately.
B. To achieve policy objective (A1), registrars should deploy (or continue to deploy) methods to support registrant-based email contact (See section 2.1.2 discussion of the two methods). The SSAC further recommends uniform requirements for safeguards be developed for the registrant-based email contact. The requirements should include maintaining the privacy of the registrant as appropriate and service level commitments to set expectations for the use of the service. These safeguards are independent of the method chosen (e.g., unique email addresses or web-based forms).
C. To achieve policy objective (A2), additional research is needed on the methods, their efficacy, and their tradeoffs. We recommend the EPDP Phase 2A *not* specify a method for correlating registrations with a common contact at this time.

[10] See SAC104, section 3.6. https://www.icann.org/en/system/files/files/sac-104-en.pdf