EPDP PHASE II
OVERVIEW OF THE INITIAL FINAL REPORT

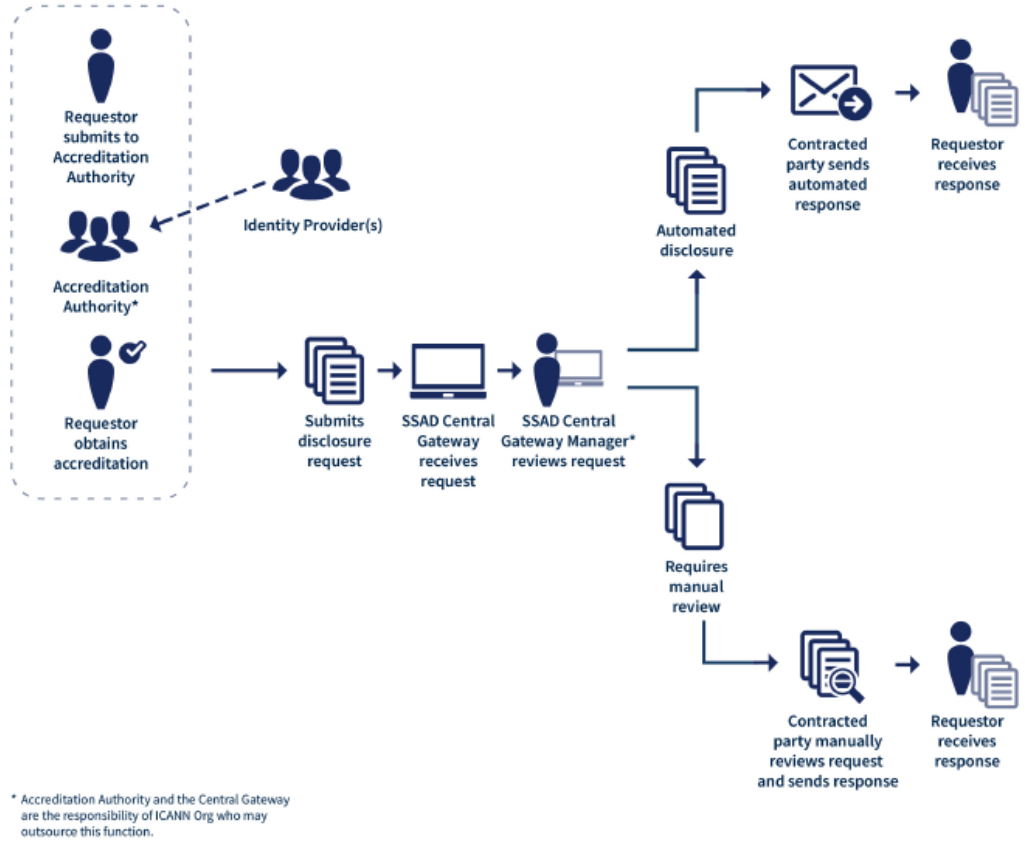
FEBRUARY 2, 2020

Alan Greenberg
&
Hadia Elminiawi

TOPICS

- SSAD model put forward for public comment
- EPDP phase 2 recommendations brief

SSAD MODEL PUT FORWARD FOR PUBLIC COMMENT



SSAD MODEL PUT FORWARD FOR PUBLIC COMMENT

SSAD anticipated benefits

- Single Location to submit requests
- Standardized requests forms
- Built in authentication process
- Standardized review and response process

EPDP PHASE 2 RECOMMENDATIONS BRIEF

	Recommendation	Brief
1	Accreditation	• SSAD MUST only accept requests from accredited organizations or individuals. • The accreditation requirements MAY differ (between regular users and one time users) • An individual accessing SSAD using the credentials of an accredited entity (e.g. legal persons) warrants that the individual is acting on the authority of the accredited entity. • The accreditation policy defines a single Accreditation Authority, managed by ICANN org. • This accreditation authority MAY work with external or third-party Identity Providers. • Decision to authorize disclosure will reside with Registrar, Registry or the Central Gateway Manager, as applicable based on the identity credential, signed assertion, and required data. • The presence of these credentials alone DOES NOT result in or mandate an automatic access/disclosure authorization. • The ability to automate decision making is possible under certain circumstances where lawful. • Accreditation Authority must define a dispute resolution and complaints process. • MUST be audited by an auditor on a regular basis. In case of repeated failure to comply a new accreditation authority must be created. • Accredited entities must be audited for compliance with accreditation policies. • the Accreditation Authority can revoke the accredited user's status as an accredited user of the SSAD. • The accreditation will be a service that is financially sustainable.
2	Accreditation of governmental entities	• Accreditation by a countries'/territories' government body or its authorized body would be available to various eligible government entities that require access to nonpublic registration data for the exercise of their public policy task. • Whether an entity should be eligible is determined by a country/territory nominated Accreditation Authority. • Accreditation does not guarantee disclosure of the data. The final responsibility for the decision to disclose data lies with the data controller

EPDP PHASE 2 RECOMMENDATIONS BRIEF

	Recommendation	Brief
3	Criteria and Content of Requests	• The objective of this recommendation is to allow for the standardized submission of requested data elements, including any supporting documentation. • Requests include a request type (e.g. urgent)
4	Third Party Purposes/Justifications	• Third parties may submit data disclosure requests for specific purposes such as: (i) criminal law enforcement, national or public security, (ii) non law enforcement investigations and civil claims, including, intellectual property infringement and UDRP and URS claims, (iii) consumer protection, abuse prevention, digital service provider (DSP) and network security • Assertion of one of these specified purposes does not guarantee access
5	Acknowledgement of receipt	• Receipt of a SSAD request by the Central Gateway Manager MUST be without undue delay. • The Central Gateway Manager MUST confirm that all required information is provided. • Should the Central Gateway Manager determine that the request is incomplete, the Gateway Manager MUST reply to the requestor with an incomplete request response, detailing which required data is missing • The Central Gateway must provide an opportunity for the requestor to amend its request. • The Central Gateway response should include information about the subsequent steps as well as the timeline consistent with the **recommendations outlined below.**

EPDP PHASE 2 RECOMMENDATIONS BRIEF

	Recommendation	Brief
6	Contracted Party Authorization	• The CP to which the disclosure request has been routed MUST review every request on its merits. • MUST NOT disclose data on the basis of accredited user category alone • Automated review is not explicitly prohibited where it is both legally and technically permissible. • CP MAY outsource the authorization responsibility to a third-party provider, but the Contracted Party will remain ultimately responsible for ensuring that the applicable requirements are met. • The Contracted Party MUST make the final determination of the appropriate lawful basis for the Contracted Party to disclose the requested information. • The Contracted Party SHOULD make a threshold determination (without considering the underlying data) about the legitimacy and necessity of the request, accordingly the requester may deny the request or ask for further information. • Once the validity of the request is determined under point 6 (bullet 4)above. The CP review of the underlying data SHOULD assess at least: ● Does the data requested contain personal data? ● The applicable lawful basis. The Contracted Party determines if the balancing test, similar to the requirements under GDPR's 6.1.f, and as described in the report below, is applicable and proceed accordingly.

EPDP PHASE 2 RECOMMENDATIONS BRIEF

	Recommendation	Brief
7	Authorization for automated disclosure requests	• This recommendation concerns disclosure requests for which it has been determined that these can be responded to in an automatic fashion (i.e. no human intervention required). • The Central Gateway Manager MUST confirm that all required information as per rec#3 is provided and that the request meets the criteria established in these policy recommendations (and is confirmed during the implementation phase) to qualify as an automated disclosure request. • With respect to disclosure requests that would be sent to a Contracted Party for manual evaluation, a Contracted Party MAY request the Central Gateway to fully automate all, or certain types of, disclosure requests. • A Contracted Party MAY retract or revise a request for automation that is not required by these policy recommendations at any time.
8	Response Requirements	1. **For the Central Gateway:** • MUST confirm that all required information is provided. • Should the Central Gateway Manager establish that the request is incomplete, the Central Gateway Manager MUST provide an opportunity for the requestor to amend and resubmit its request. • Following confirmation that the request is syntactically correct and that all required information has been provided, the Central Gateway Manager MUST immediately and synchronously respond with an acknowledgement response and relay the disclosure request to the responsible CP, if it does not concern a request that meets the criteria for automatic disclosure. • As part of its relay to the responsible CP, the Central Gateway Manager MAY provide a recommendation to the CP whether to disclose or not. • The CP MAY follow this recommendation. If the Contracted Party decides not to follow the recommendation of the Central Gateway Manager, the Contracted Party MUST communicate its reasons for not following it, which enables the central gateway to learn an improve.

EPDP PHASE 2 RECOMMENDATIONS BRIEF

	Recommendation	Brief
8	Response Requirements (continued)	**2. For Contracted Parties** • MUST provide a disclosure response without undue delay, unless there are exceptional circumstances. Such exceptional circumstances MAY include the overall number of requests received if the number far exceeds the established SLAs. • SSAD requests that meet the automatic response criteria must receive an automatic disclosure response. • For requests that do not meet the automatic response criteria, a response MUST be received in line with the SLAs outlined. • Responses where disclosure of data (in whole or in part) has been denied MUST include: rationale sufficient for the requestor to understand the reasons for the decision, Additionally, in its response, the entity receiving the access/disclosure request MUST include information on how public registration data can be obtained. **3. Urgent SSAD Requests** • A separate accelerated timeline has been recommended for the response to 'Urgent' SSAD Requests. • The criteria to determine whether it concerns an urgent request are limited to circumstances that pose an imminent threat to life, serious bodily injury, critical infrastructure (online and offline) or child exploitation. • the use of 'Urgent' SSAD Requests is not limited to LEA. • Abuse of urgent SSAD requests: repeated violations may result in the Central Gateway Manager suspending the ability to make urgent requests via the SSAD. • Contracted Parties MUST maintain a dedicated contact for dealing with Urgent SSAD Requests which can be stored and used by the Central Gateway Manager, in circumstances where an SSAD request has been flagged as Urgent • CPs MUST publish their standard business hours and accompanying time zone in the SSAD EPDP Team Phase 2 Initial Report 7 February 2020 Page 31 of 114 portal15 (or in another standardized place that may be designated by ICANN from time to time) • If the CP determines that disclosure would be in violation of applicable laws or result in inconsistency with these policy recommendations, the CP MUST document the rationale and communicate this information to the requestor and ICANN Compliance (if requested). • The requestor MAY be file a compliant with ICANN Compliance.

EPDP PHASE 2 RECOMMENDATIONS BRIEF

	Recommendation	Brief
9	Determining Variable SLAs for response times for SSAD	**The proposed matrix and accompanying text represents a starting proposal to gather community feedback** • The initial priority of a disclosure request is set by the requestor, using the priority options provided by the Central Gateway Manager • It is possible that the initially-set priority may need to be reassigned during the review of the request. • Within the defined response times, the CP SHALL respond to the request. • Urgent Requests, priority1, 1 business day / 85% / 90% / 95% • Administrative proceedings (such as response to UDRP filing) priority2, 2 business days / 85% / 90% / 95% • All other requests prority3, according to the following: **Phase 1** begins six (6) months following the SSAD Policy Effective Date. **Phase 2** begins one (1) year following the SSAD Policy Effective Date. In Phase 1, registrar response targets for SSAD Priority 3 requests will be five (5) business days In Phase 2, Contracted Party compliance targets for SSAD Priority 3 requests will be ten (10) business days
10	Acceptable Use Policy	**The requestor:** • MAY request data from the SSAD for multiple purposes per request, for the same set of data requested. • For each stated purpose must provide (i) representation regarding the intended use of the requested data and (ii) representation that the requestor will only process the data for the stated purpose(s). • MUST, for each request for RDS data, provide representations of the corresponding purpose and lawful basis for the processing.

EPDP PHASE 2 RECOMMENDATIONS BRIEF

	Recommendation	Brief
11	Disclosure Requirement	**CPs and SSAD** • MUST log requests. • Where required by applicable law, MUST perform a balancing test before processing the data. • MUST disclose to the Registered Name Holder (data subject), on reasonable request, confirmation of the processing of personal data relating to them, per applicable law. • Where required by applicable law, MUST provide mechanism under which the data subject may exercise its right to erasure and any other applicable rights. • CP should provide notice to data subjects of the types of entities/third parties which may process their data • ICANN and the CPs will draft and agree upon a privacy policy for the SSAD and standard language (relating to the SSAD) to inform data subjects according to Art. 13 and 14 GDPR
12	Query Policy	**The Central Gateway Manager:** • MUST monitor the system and take appropriate action, such as revoking or limiting access, to protect misuse of the system • 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. • MUST respond only to requests for a specific domain name and MUST examine each request on its own merits. **The SSAD Must** • Support requests keyed on fully qualified domain names (without wildcards). • Support the ability of a requestor to submit multiple domain names in a single request. • Route each domain individually to the entity responsible for the disclosure decision • Consider each request on its own merits. • Only support requests for current data

EPDP PHASE 2 RECOMMENDATIONS BRIEF

	Recommendation	Brief
13	Terms of use	• Appropriate agreements, such as terms of use for the SSAD, a privacy policy and a disclosure agreement are put in place that take into account the report recommendations. • These agreements are expected to be developed and negotiated by the parties involved in SSAD.
14	Retention and Destruction of Data	**Requestors** • MUST confirm that they will store, protect and dispose of the registration data in accordance with applicable law. • MUST retain only the gTLD registration data for as long as necessary to achieve the purpose stated in the disclosure request.
15	Financial Sustainability	• The costs for developing, deployment and operationalizing the system, to be initially borne by ICANN org, Contracted Parties and other parties that may be involved. • The subsequent running of the system is expected to happen on a cost recovery basis. • The costs associated with becoming accredited would be borne by those seeking accreditation. • Fees associated with using the SSAD may differ for users based on request volume or user type among other potential factors. • The objective is that the SSAD is financially self-sufficient without causing any additional fees for registrants • Requestors of the SSAD data should primarily bear the costs of maintaining this system. • ICANN MAY contribute to the (partial) covering of costs for maintaining the Central Gateway. • The SSAD SHOULD NOT be considered a profit-generating platform for ICANN or the contracted parties • Funding for the SSAD should be sufficient to cover costs, including for subcontractors at fair market value and to establish a legal risk fund. • Accreditation applicants MAY be charged a to-be-determined non-refundable fee proportional to the cost of validating an application. b) Rejected applicants MAY re-apply, but the new application(s) MAY be subject to the application fee. c) Fees are to be established by the accreditation authority. d) Accredited users and organizations MUST renew their accreditation periodically.

EPDP PHASE 2 RECOMMENDATIONS BRIEF

	Recommendation	Brief
16	Automation	• Receipt, authentication and transmission of SSAD requests be fully automated insofar as it is technically feasible. • Disclosure decisions SHOULD be automated only where technically and commercially feasible20 and legally permissible. • In areas where automation does not meet these criteria, standardization of disclosure decisions is the baseline objective. • Intake of requests, credential check, request submission validation (format & completeness, not content) could be automated, while it may not be possible to completely automate all request review and disclosure the SSAD MUST allow for the automation of syntax checking of incoming requests, resulting in an automatic response that indicates the errors to the requestor. This automation addresses the risk of filling up the request queues of the discloser with malformed request • The SSAD MUST allow for the automation of checking that the contents of a request is complete, per policy, resulting in an automatic response that provides details explaining what elements are incomplete. • The SSAD MUST allow for the automation of an immediate response that indicates the receipt of a valid request and some indication that it will be processed. Typically, such responses include a "ticket number" • The SSAD MUST allow for automation of the processing of well-formed, valid, complete, properly-identified requests from accredited users with some limited and specific set of legal basis and data processing purposes. These requests MAY be automatically processed and result in the disclosure of non-public RDS data without human intervention.
17	Logging	The logging requirements will cover: ● Accreditation authority ● Central Gateway Manager ● Identity provider ● Contracted Parties ● Activity of accredited users such as login attempts, queries ● What queries and disclosure decision(s) are made

EPDP PHASE 2 RECOMMENDATIONS BRIEF

	Recommendation	Brief
18	Audits	• As part of any audit, the auditor MUST be subject to reasonable confidentiality obligations with respect to proprietary processes and personal information disclosed during the audit. • **Audits of Identity Provider(s)** MUST be audited periodically • **Audits of Accredited Entities/Individuals** Appropriate mechanisms MUST be developed in the implementation phase to ensure accredited entities' and individuals' compliance with the policy requirements as defined in the accreditation preliminary recommendation • **Audits of the Accrediting Authority** If ICANN outsources the accreditation authority function to a qualified third party, the accrediting authority MUST be audited periodically ICANN org as the Accreditation Authority is not required to audit governmental entities As ICANN serves as the accreditation authority, existing accountability mechanisms are expected to address any breaches of the accreditation policy
19	Mechanism for the evolution of SSAD	The creation of a Mechanism for the evolution of SSAD that has the responsibility to provide guidance on: a) SLA matrix review; b) Categories of disclosure requests which should be automated; c) Other implementation improvements such as the identification of possible user categories and/or disclosure rationales. The EPDP Team will further consider the details of the Mechanism, and would like request community input on the following • What existing processes / procedures, if any, can be used to meet the above responsibilities? • If no suitable existing processes / procedures can be used, what type of mechanism should be created? • How is guidance of the Mechanism expected to be implemented? charter for the Mechanism is expected to be developed during the implementation phase

THANK YOU - QUESTIONS?

Alan Greenberg
&
Hadia Elminiawi