**Public Comment Review Tool – EPDP-P2 – Initial Report**

Updated 27 March 2020

# RECOMMENDATION 1

| **#** | **Comment** | **Contributor** | **EPDP Response / Action Taken** |
| --- | --- | --- | --- |
| The EPDP Team recommends that a policy for accreditation of SSAD users is established. | | | |
| **Support Recommendation as written** | | | |
|  | No Comment | Georgia Institute of Technology, BIOFARMA, AXA - Eirini Patsi, Article 19, SSAC, GAC | Support  **EPDP Response:** Thank you for the support.  **Action Taken:** None.  [**COMPLETED**] – None |
|  | MarkMonitor supports the concept of accreditation and encourages the SSAD to allow for the upfront establishment of as many accreditation attributes upfront as possible. These attributes should include identity characteristics, legal rights, law enforcement status, etc. as they may pertain to the accredited requestor. Enabling these attributes to be established upfront should ensure that subsequent data requests are automated as much as possible, and manually processed as quickly and uniformly as possible where necessary. | MarkMonitor | Support  **EPDP Response:** Thank you for the support.  **Action Taken:** None.  [**COMPLETED**] – None |
| **Support Recommendation intent with wording change** | | | |
|  | Fees: The accreditation service will be a service that is financially sustainable and not dissuasive to any category of requestor. | VKGP SA dba Vanksen | Support  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
|  | MPA recommends adding to the Accreditation Recommendation, and to the SSAD, the concept of Trusted Notifiers. Trusted Notifiers would be entities or individuals with recognized subject matter expertise who would undergo additional scrutiny, either at the time they are initially accredited and/or in an ongoing manner, to recognize or establish their accuracy and their track record of good faith and compliant use of the SSAD in support of their work monitoring, investigating and acting against specific use cases of illegal activity and domain abuse. | Motion Picture Association | Support  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
|  | The Accreditation Authority: (m) User groups/categories referred to should be better defined. Does it mean Companies, Not-Profits, individuals, etc.?  Accredited entities or individuals: "store, protect and dispose of the gTLD registration data..." should this say gTLD registration data or simply "registration data"? What about ccTLD's? | Pernod Ricard | Support  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
|  | - The Accreditation Authority must be defined  - It is not defined in what case the Accreditation Authority may work with external or third-party Identity Providers | ANDEMA | Support  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
|  | While fully supporting the premise that there be an accreditation policy for SSAD users, we would prefer more clarity on the Identity Providers. For example, for trade mark issues, given their global mandate and access to trade mark registries/databases, we strongly advocate that this task should fall to WIPO.  Under “implementation guidance” (p. 20), we believe that “information asserting trade mark ownership” should be clarified to ensure that service providers and/or lawyers acting on behalf of the trade mark owners should also be eligible for accreditation. | LEGO | Support  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
|  | The IPC supports the framework and principles outlined in this recommendation and believes it will form a solid foundation to ensure an effective, efficient and legally sound access to the SSAD system.  We believe however that it should be improved to include the concept of an Accredited Entity who is also a Trusted Notifier. Accredited Entities who are also Trusted Notifiers are subject matter experts that have been additionally vetted to monitor and investigate issues of illegal activity and abuse. Befitting their designation, Accredited Entities who have been vetted to be a Trusted Notifier have an established reputation for accuracy, a recognized relationship with the ecosystem and a proven record of following the defined process for requesting access to non-public Registration Data via the SSAD.  The accreditation period should be as long as possible, to reduce the burden of having to frequently seek re-accreditation.  There should be a specified appeal mechanism for any decisions to de-accredit an accredited user on the basis of an alleged violation of the system. | IPC | Support  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
|  | No assurance of Whois data accuracy is enumerated, and this threatens to disrupt the integrity of Whois at the outset. Though neither GDPR nor any other law protects fake data, this report shirks the responsibility of ensuring accuracy as part of an accountable and effective Whois framework.  Based on the Implementation Guidance that concludes Recommendation #1, the EPDP clearly recognizes the importance of accuracy and accountability for accreditation applicants that will be required to present “a business registration number and the name of the authority that issued this number,” along with “information asserting trademark ownership”. A significant proportion of Whois data is inaccurate and the absence of an accuracy and accountability framework for that data set contradicts the principles the EPDP seeks to establish for the SSAD accreditation policy as well as the principles of GDPR itself: as the GAC and ALAC stated in their joint Statement on the EPDP: “In accordance with  Article 5 of the GDPR, every reasonable step must be taken to ensure the accuracy of the data in view of the purposes for which it is processed.”  While specific suggestions are outlined below, the BC adds here that the EPDP team’s recommendations can be improved by including the concept of an Accredited Entity who is also a Trusted Notifier. Accredited Entities who are also Trusted Notifiers would be subject matter experts that have been additionally vetted to monitor and investigate issues of illegal activity and abuse. Trusted Notifiers would have an established reputation for accuracy, a recognized relationship with the ecosystem and a proven record of following the defined process for requesting access to non-public Registration Data via the SSAD.  Principle d): The BC prefers that disclosure decisions be automated/centralized to the greatest extent possible and limit to the greatest extent possible the number of individualized disclosure decisions being made by individual registry operators and registrars. Further, the BC supports that references to “registrar,” “registry,” and “central gateway manager” be changed to “Controller,” as that is what GDPR requires. Limiting to “Controller” would allow the recommendation to scale according to the ultimate decision on who the “Controller” is in this scenario.  Principle h): The report should define which types of requests could be responded to in an automated manner. For purposes of disclosure, the BC supports automated or quasi-automated (i.e. human review by the central managing authority for provision of required information) access/disclosure decisions in cases of well-founded allegations of abuse (e.g., cybersquatting, phishing, trademark or copyright infringement, etc.), as evidenced in the assertions and supporting materials produced in connection with same/with the disclosure request itself.  Principle i): Does the referred-to code of conduct comply with Art. 40 of the GDPR and will it contain mechanisms which enable the body referred to in Art. 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it? Further, how is the Accreditation Authority the “authority” on the proper application of data protection laws? The report should clarify.  Principle j): The BC poses the following:  Regarding the definition of eligibility requirements for accredited users, will this be reviewed and revised over time with learnings from the accreditation process? Preliminary eligibility requirements may be unnecessarily exclusive.  Regarding identity credential revocation procedures, there must be an appeal or escalation process enumerated.  Regarding “requirements beyond the baseline listed [above] may be necessary for certain classes of requestors,” these should be available to applicants prior to application.  Principle k): This language should be sharpened to be more specific, if in fact it refers to an appeal or escalation process. Such a mechanism must include due process checks and balances.  Principle l): In addition to accredited authorities being audited for compliance, so should the accreditation provider to ensure compliance with timely and reasonable accreditation grants. The report also should detail how often the audits should occur.  Principle n): The cadence of reports “on a regular basis” should be enumerated.  Principle o): “Abuse of the system” should be defined and differentiated (if applicable) from violation of the code of conduct.  Principle p): Regarding “abuse of the system,” the report should also identify who supervises the accreditation authority in the instance of “abuse” on its part (e.g., over-restrictive granting of credentials or arbitrary revocation of credentials).  Principle q): While the BC appreciates the notion of graduated penalties, again here, there should be included an appeal or escalation process in the event of a dispute over penalties or potential revocation.  Principle r): Will graduated sanctions be enumerated in advance? Will graduated sanctions be uniform across all accreditation authorities? There may be entities seeking accreditation from multiple providers.  Principle t): Again here, an appeal mechanism should be included.  Principle u): The BC poses the following:  Regarding “prevent abuse of data received,” the term “abuse” should be defined.  Regarding “de-accreditation if they are found to abuse use of data,” due process and checks and balances should be required.  Principle v): Regarding a “demonstrable threat to the SSAD,” the BC advises there needs to be a definition and metric so that decisions are objective and not subjective.  Regarding fees, the BC recommends updating the language of that recommendation to read: The accreditation service will be a not-for-profit service that is financially sustainable.  Regarding implementation guidance, the BC offers the following:  a): “Recognized, applicable and well-established organizations” needs definition as it applies to supporting the Accreditation Authority. Also, the recommendation does not identify who would provide “vetting” as it applies to Recommendation j [above].  b): “Information asserting trademark ownership” could be clarified – does this refer to information demonstrating ownership of a trademark by the accredited party or that the accredited party is acting on behalf of a trademark owner (or both)? What kinds of information would this entail? A copy of TM registration / certificate? Power of Attorney or other form demonstrating agency?  d): When the team recommends that “logged data SHALL only be disclosed, or otherwise made available for review,” by whom is the review conducted? Is this part of a formal process? This needs clarification. | BC | Support  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
|  | While fully supporting the premise that there be an accreditation policy for SSAD users, we would prefer more clarity on the Identity Providers. For example, for trade mark issues, given its global mandate and access to trade mark registries/databases, we strongly advocate that this task should fall to WIPO.  Under “implementation guidance”, we believe that “information asserting trade mark ownership” should be clarified to ensure that service providers and/or lawyers acting on behalf of trade mark owners should also be eligible for accreditation. | AIM - European Brands Association | Support  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
|  | Where it is noted: “SSAD MUST only accept requests for access/disclosure from accredited organizations and individuals”; the terms “companies, associations” shall be added in order to explicitly include the participation of all types of legal persons in this process.  In addition, there is no guarantee of the accuracy of WHOIS data listed. This put at risk from the beginning the validity of WHOIS. Neither the GDPR nor any other law projects fake data. But, since we know from experience that WHOIS data is often inexact, this report should also aim at ensuring correctness of WHOIS.  As the GAC and ALAC stated in their joint Statement on the EPDP: “In accordance with Article 5 of the GDPR, every reasonable step must be taken to ensure the accuracy of the data in view of the purposes for which it is processed.” | Novartis,Hermes International,French Anticounterfeiting Committee,Comité Colbert,SERVIER,SOMFY ACTIVITES SA,Belgian Association Anti-Counterfeiting,CHANEL,UNIFAB,Sanofi | Support  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
|  | At the outset, we would like to flag our overarching comments given in response to Q46.  Marques supports the intent behind recommendation #2, but is concerned by the lack of any specificity and detail in key areas. There appears to be an expectation that that this detail will be fleshed-out by the later implementation team, or even by the Accreditation Authority itself – even this presently seems ambiguous and unclear.  Examples of areas where there is ambiguity and/or greater clarity would benefit:  • Signed assertions (g) are listed under the “Requirements of the Accreditation Authority”. Certainly, the Accreditation Authority needs to be able to manage such assertions, but the information to be provided by a party seeking accreditation should be grouped in one place.  • The signed assertions required for a one-off basis versus a regular user are unclear and some appear to relate rather to a specific SSAD request. E.g. the “trademark ownership/registration” information is potentially case-specific. The process will need to allow for a user to be accredited and then to associate additional rights to their existing accreditation on an ongoing basis, as required. The “purpose of the request” and “legal basis of the requestor” would also seem to have the potential to be case-specific  • What precisely are these assertions? E.g. Is it expected that there will be a set of declarations such as “to comply with the law on storage/retention” or will there be an actual set of standards as to how that retention is to be effected and the maximum length of time that the data may be store? Who will be making that decision? As drafted, it appears this may simply be left to the Accreditation Authority – if that is the intent, this seems unwise since this is a contentious area.  • Paragraph (i) is also listed under “Requirements of the Accreditation Authority” and refers to a base line “code of conduct”. This also appears to imply that the creation of the code of conduct is this being left to the Accreditation Authority, and although there is a mention of the need for a description of the extent of stakeholder consultation this falls short of an actual obligation to consult. Since breach of the code of conduct can have serious implications for an accredited user (o) there must be a proper consultative process.  • Lack of any specificity as to the dispute resolution and complaints process (k).  • Lack of specificity as to the graduated penalties for a user (q). Where is it envisaged that the responsibility for developing this will lie? Since different community interests will have strong and opposing views on how such a graduated process should apply, this needs to be expanded-upon.  • What is a “demonstrable threat to the SSAD” (v) and who is determining this? This should not be a unilateral decision of the Accreditation Authority, there should be some agreed boundaries.  Review and update definitions and provide a full set of definitions for the Policy in one place: Prior to the publication of the Final Report it would be beneficial to review and ensure all terms which are being used as defined terms within the Policy are captured in a single “Definitions” section. Presently, some later recommendations include the addition of new definitions, and some terms which appear to be intended as defined terms are not so defined. For example, the term “Requestor” is capitalised and used within definition of “Authentication”, but is not separately defined. Elsewhere, it is used without capitalisation. This should be standardised as part of the clean-up of the Final Report. | MARQUES | Support  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
|  | Accreditation is an important element of the SSAD as it saves the time and effort required by decision-making entities to verify the requestor, provides external assurance that the requestors have been verified and reduces the load on the SSAD. However, the ALAC is concerned that given the fact that requests to SSAD can only be submitted by accredited users, the accreditation process could end up being a bottle neck, limiting access to the system. We therefore see that the accreditation entity in addition to having a uniform baseline application procedure and accompanying requirements should also have a clear timeline for its process and response. | ALAC | Support  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
|  | Whilst we do support the intent behind recommendation #2, much of the detail does seem to be left for future implementation work. Some of this seems quite fundamental to what the actual policy for operation of an SSAD will be and it would be preferable to have this detail worked out before adopting recommendations, for example:  • How the accreditation of a single user and a regular user might differ. The recommendation states that this MAY be the case, but it would be preferable to have clarity on whether this will be the case.  • The code of conduct  • Dispute resolution and complaints processes  • Graduated penalties for users  • What constitutes a “demonstrable threat to the SSAD”  The recommendation as currently drafted also somewhat lacks clarity for those not participating in the detailed work of the working group. For example:  • Does an individual accessing the SSAD on behalf of an accredited legal person also have to be separately accredited?  • Some of the signed assertions appear to go to the facts of a specific request rather than being for the accreditation of a user. Greater explanation/detail would help to clarify.  • Are the assertions regarding compliance with law, storage, protection, retention/disposal, use of the data for legitimate and lawful purposes, prevention of abuse, auditing, and so on intended to be a simple set of statements/declarations to that effect; will there be a set of minimum standards that they must acknowledge compliance with; or is the requesting user expected to identify the exact manner in which they will meet these various assertions? | Com Laude Group | Support  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
|  | The definition for “Accreditation” refers to a user being approved to gain access to the SSAD; this should be reworded as there is no non-public registration data contained in SSAD to access, and “accreditation” should instead refer to the user eligibility for making disclosure requests.  The recommendation includes credentials for an entity (organization) used by several individuals employed there, that is bad security practice. Individual users should be accredited.  Who is going to build an accreditation service that complies with these byzantine requirements? The implementation will be a significant amount of work and likely expensive  Recommendation 2 is better formatted to explain the accreditation process and reasoning behind it, so maybe Rec 1 can be adjusted to align with Rec 2 (same section categories, etc) | RrSG | Support  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
|  | The INTA recommends the following revisions to the working definitions in Recommendation #1:  Authentication - The process or action of Validating the Identity Credential and Signed Assertions of a Requestor. [ INTA notes that the term “Requestor” is not defined anywhere and appears inconsistently in initial cap or all lower case. Should be defined in this section. We suggest a specific definition for this term below.]  Authorization - A process for approving or denying disclosure of non-public registration data.  De-accreditation of Accreditation Authority – An administrative action by which ICANN org revokes the agreement with the accreditation authority, if this function is outsourced to a third party, following which it is no longer approved to operate as the accreditation authority. [Moved this definition to appear in alphabetical order.]   * “Identifier Credential: A data object that is a portable representation of the association between an identifier and a unit of authentication information, and that can be presented for use in Validating an identity claimed by an entity that attempts to access a system. Example: Username/Password, OpenID credential, X.509 public-key certificate. * [We suggest reordering these definitions so they appear in alphabetical order.] * Identity Provider - Responsible for 1) Verifying the identity of a requestor and managing an Identifier Credential associated with the requestor and 2) Verifying and managing Signed Assertions associated with the Identifier Credential. For the purpose of the SSAD, the Identity Provider may be the Accreditation Authority itself or it may rely on zero or more third parties. * Requestor – An individual or organization seeking access to non-public domain name registration data through the SSAD. * Revocation of User Credentials- The event that occurs when an Identity Provider declares that a previously valid credential has become invalid. * Signed Assertion - A data object that is a portable representation of the association between an Identifier Credential and one or more access assertions, and that can be presented for use in Validating those assertions for an entity that attempts such access. Example: [OAuth credential], X.509 attribute certificate. [Moved to appear in alphabetical order.]   INTA COMMENTS:  The definitions have been only revised slightly and placed in alphabetical order but in general should be expanded significantly to include many additional terms used in the policy text below, as found in the EPDP Phase 2 Team working definitions available in the ICANN documents linked to the Initial Report. The EPDP Phase 2 team’s working definitions, which include draft definitions for terms such as “Legitimate Interest”, “Right of Access”, “Disclosure” would be helpful here. The above definitions appear to come from different sources and take different approaches to defining the components of the SSAD. Some have a legal context or approach (e.g., third parties, signed assertions), while others employ terms typically identified with automation, computing systems or even mathematics (e.g., data object, construct, a value, truth). Many employ terms treated as defined terms (e.g., “Requestor”, “Discloser”) that are not defined here but should be. A proposed definition for Requestor has been inserted based on its use in other definitions above and incorporating the related terms from those definitions in which Requestor was used. It would also be useful to see how SSAD and these terms relate to the existing WhoIs system, perhaps making reference to data objects currently used (e.g., registrant, registrant organization) and how they would be accessed and disclosed under SSAD.  The EPDP Team recommends that a policy for accreditation of SSAD users is established. The following principles underpin the accreditation policy:  a) SSAD MUST only accept requests for access/disclosure from accredited organizations or individuals. However, accreditation requirements MUST accommodate any intended user of the system, including an individual or organization who makes a single request. The accreditation requirements for regular users of the system and a one-time user of the system MAY differ. [Comment: Any differences in such requirements should be provided by the EPDP along with rationale.]  b) Both legal entities and/or individuals are eligible for accreditation. 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.11 [Comment: Are the individuals identified in the signed assertions or are the warranties separate documents or assertions?]  c) The Accreditation policy defines a single Accreditation Authority, managed by ICANN org. This Accreditation Authority MAY work with external or third-party Identity Providers that could serve as clearinghouses to Verify identity and authorization information associated with those requesting accreditation.  d) The decision to authorize disclosure of non-public registration data, based on Validation of the Identity Credential, Signed Assertions, and data as required in preliminary recommendations concerning criteria and content of requests, will reside with the Registrar, Registry or the Central Gateway Manager, as applicable. [Comment: Are these delineated sufficiently in the referenced recommendations; is the decision resident with each of the contract parties listed separate or co-dependent. Need to clarify or link to the recommendations that show which aspects of the authorization decision reside with the Rr, which with the Ry and which with the CGM/ICANN. It should be clarified whether requests will initially be routed to the Rr or Ry or both, or responded to automatically by the CGM where possible.]  Requirements of the Accreditation Authority  e) Verifying the Identity of the Requestor: The Accreditation Authority MUST verify the identity of the Requestor, resulting in an Identity Credential.  f) Management of Signed Assertions: The Accreditation Authority MUST verify and manage a set of dynamic assertions/claims associated with and bound to the Identity Credential of the Requestor. This Verification, performed by an Identity Provider, results in a Signed Assertion.  g) Signed Assertions convey information such as:  o Assertion as to the purpose(s) of the request  o Assertion as to the legal basis of the Requestor  o Assertion that the user identified by the Identity Credential is affiliated with the relevant organization [Comment: Is this one Requestor in which an individual is part of the Requestor due to the affiliation, e.g. an Authorized Representative, or are each of the individual and the entity authorized as separate Requestors? This should be clarified.]  o Assertion regarding compliance with laws (e.g., storage, protection and retention/disposal of data) [Comment: Will these be provided as standards agreed upon under GDPR or identified based on ICANN policy? Will it be a general assertion to comply with applicable laws or will there be more specific compliance requirements provided?]  o Assertion regarding agreement to use the disclosed data for the legitimate and lawful purposes stated [Comment: Will there be a standard set of warranties developed that apply to all users equally, or will there be distinctions based on entity versus individual, or some other status, such as private sector, government, law enforcement, etc.?]  o Assertion regarding adherence to safeguards and/or terms of service and to be subject to revocation if they are found to be in violation  o Assertions regarding prevention of abuse, auditing requirements, dispute resolution and complaints process, etc.  o Assertions specific to the status of the specific Requestor – trademark ownership/registration for example [Comment: Will documents or written evidence have to be submitted or are signed assertions sufficient?]  o Power of Attorney statements, when/if applicable. [Comment: when will such PoA statements be required/applicable? For any user acting on behalf of another party? Only for qualified legal counsel?]  h) Validation of Identity Credentials and Signed Assertion, in addition to the information contained in the request, to facilitate the decision of the authorization provider to accept or reject the Authorization of an SSAD request. For the avoidance of doubt, the presence of these credentials alone DOES NOT result in or mandate an automatic access / disclosure authorization. However, the ability to automate access/disclosure authorization decision making is possible under certain circumstances where lawful. [Comment: What does this mean, under which circumstances and compliance with which law according to which decision maker? In which circumstances? For purposes of disclosure, INTA would strongly support automated or quasi-automated (i.e. human review by the central managing authority for provision of required info) access/disclosure decisions in cases of well-founded allegations of cybersquatting, trademark or copyright infringement, as evidenced in the assertions and supporting materials produced in connection with same/with the disclosure request itself. Other comments regarding automation are provided below.]  i) Defines a baseline “code of conduct”12 that establishes a set of rules that contribute to the proper application of data protection laws - including the GDPR, including:  o A clear and concise explanatory statement.  o A defined scope that determines the processing operations covered (the focus for SSAD would be on the Disclosure operation.)  o The mechanism that allows for the monitoring of compliance with the provisions.  o Identification of an Accreditation Body Auditor (a.k.a. monitoring body) and definition of mechanism(s) which enable that body to carry out its functions.  o Description as to the extent a “consultation” with stakeholders has been carried out.  The Accreditation Authority:  j) MUST have a uniform baseline application procedure and accompanying requirements for all applicants requesting Accreditation, including:  o Definition of eligibility requirements for accredited users  o Identity Validation Procedures  o Identity Credential Management Policies: lifetime/expiration, renewal frequency, security properties (password or key policies/strength), etc. [Comment: INTA would prefer longer lifetime/periods for accreditation (subject to audit) and no/low cost accreditation / cost recovery model.]  o Identity Credential Revocation Procedures: circumstances for revocation, revocation mechanism(s), etc. [see also “Accredited User Revocation & abuse section below]  o Signed Assertions Management: lifetime/expiration, renewal frequency, etc.  o NOTE: requirements beyond the baseline listed above may be necessary for certain classes of requestors.  k) MUST define a dispute resolution and complaints process to challenge actions taken by the Accreditation Authority.  l) MUST be audited by an auditor on a regular basis. [Comment: How often? This should be defined more specifically.] Should the Accreditation Authority be found in breach of the accreditation policy and requirements, it will be given an opportunity to address the breach, but in cases of repeated failure, a new Accreditation Authority must be identified or created. Additionally, accredited entities MUST be audited for compliance with the accreditation policy and requirements on a regular basis; (Note: detailed information regarding auditing requirements can be found in the Auditing preliminary recommendation).  m) MAY develop user groups / categories to facilitate the accreditation process as all Requestors will need to be accredited, and accreditation will include identity verification.  n) MUST report publicly and on a regular basis on the number of accreditation requests received, accreditation requests approved/renewed, accreditations denied, accreditations revoked, complaints received and information about the identity providers it is working with.  [Comment: As this section appears to be similar in summarizing the process and features addressed above the same comments apply regarding the need for clarification of standards and consistent use of terms to follow the process.]  Accredited User Revocation & Abuse:  o) Revocation, within the context of the SSAD, means the Accreditation Authority can revoke the accredited user’s status as an accredited user of the SSAD. A non-exhaustive list of examples where revocation may apply include 1) the accredited user’s violation of the code of conduct, 2) the accredited user’s abuse of the system, 3) a change in affiliation of the accredited user, or 4) where prerequisites for accreditation no longer exist. [Comment: Per the comments above regarding the legal entity Requestor that has an affiliated individual, does a dissociation of one authorized representative automatically result in the revocation of an entity’s Accreditation? Presumably this would not be the case for the legal entity, but may be the case for the individual – but this should be clarified. In addition, we reiterate that what constitutes an abuse of the system and/or a code of conduct violation must be made explicit. How is abuse of the system defined? How does it differ from violating code of conduct? We would also suggest that the EPDP team provide further details regarding the development of a code of conduct, when and how that would take place, and whether it would be necessary to have a separate code of conduct or whether a code of conduct could be built in to the terms of use for the SSAD along with an acceptable use policy and privacy policy. Regardless, development of the code of conduct / terms should involve all SSAD stakeholders.]  p) A mechanism to report abuse committed by an accredited user MUST be provided by SSAD. Reports MUST be relayed to the Accreditation Authority for handling. [Comment: How will abuse be defined and what verification/validation process will be used to assure that a claim of abuse is valid, legitimate, etc.?]  q) The revocation policy for individuals/entities SHOULD include graduated penalties. In other words, not every violation of the system will result in Revocation; however, Revocation MAY occur if the Accreditation Authority determines that the accredited individual or entity has materially breached the conditions of its accreditation and failed to cure based on: a) a third-party verified complaint received; b) results of an audit or investigation by the Accreditation Authority or Accreditation Authority Auditor; c) any misuse or abuse of privileges afforded; d) repeated violations of the accreditation policy; e) results of audit or investigation by a DPA.  r) In the event there is a pattern or practice of abusive behavior within an entity, the credential for the entity could be suspended or revoked as part of a graduated sanction.  s) Revocation will prevent re-accreditation in the future absent special circumstances presented to the satisfaction of the Accreditation Authority. [Comment: There should be a defined appeals process for any revocation decisions.]  De-authorization of Identity Providers  t) The authorization policy for Identity providers SHOULD include graduated penalties. In other words, not every violation of the policy will result in De- authorization; however, De-authorization may occur if it has been determined that the Identity Provider has materially breached the conditions of its contract and failed to cure based on: a) a third-party complaint received; b) results of an audit or investigation by the Accreditation Auditor or auditor; c) any misuse or abuse of privileges afforded; d) repeated violations of the accreditation policy. Depending upon the nature and circumstances leading to the de-authorization of an Identity Provider, some or all of its outstanding credentials may be revoked or transitioned to a different Identity Provider.  [Comment: As there does not appear to be a process for “authorization” of an Identity Provider (which can be an Accreditation Authority), it may be helpful to clarify how that process would work to enable further comment on de-authorization of Identity Providers.  Accredited entities or individuals:  u) MUST agree to:    o only use the data for the legitimate and lawful purpose stated;  o the terms of service, in which the lawful uses of data are described;  o prevent abuse of data received;  o [cooperate with any audit or information requests as a component of an audit;] [Comment: What is the purpose of bracketed materials, are these subject to change or interim provisions? The brackets should be removed – INTA would support the inclusion of this item.]  o be subject to de-accreditation if they are found to abuse use of data or accreditation policy / requirements;  o store, protect and dispose of the gTLD registration data in accordance with applicable law;  o only retain the gTLD registration data for as long as necessary to achieve the purpose stated in the disclosure request.  v) Will not be restricted in the number of SSAD requests that can be submitted during a specific period of time, except where the accredited entity or individual poses a demonstrable threat to the SSAD. It is understood that possible limitations in SSAD’s response capacity and speed may apply. For further details see the response requirements preliminary recommendation. [Comment: Additional clarification for what would constitute a “demonstrable threat” to the SSAD should be provided.]  Fees:  The accreditation service will be a service that is financially sustainable. For further details, see the financial sustainability preliminary recommendation.  Implementation Guidance  In relation to accreditation, the EPDP Team provides the following implementation guidance:  a) Recognized, applicable, and well-established organizations could support the Accreditation Authority as an Identity Provider and/or Verify information. Proper vetting, as described in j) above, MUST take place if any such reputable and well- established organizations are to collaborate with the Accreditation Authority.  b) Examples of additional information the Accreditation Authority or Identity Provider MAY require an applicant for accreditation to provide could include:  o a business registration number and the name of the authority that issued this number (if the entity applying for accreditation is a legal person);  o information asserting trademark ownership. [Comment: This could be clarified – does this refer to information demonstrating ownership of a trademark by the accredited party or that the accredited party is acting on behalf of a trademark owner (or both)? What kinds of information would this entail? Copy of TM registration / certificate? Power of Attorney or other form demonstrating agency?]  INTA COMMENTS:  In general, INTA supports the concept of requiring additional information regarding standard and readily available electronic data regarding the active status of a trademark registration, but rights holders with valid claims to ownership or the establishment of rights based on pending applications, judicial recognition, or other evidence of common law trademark rights should not be summarily prohibited from qualifying for Accreditation through verifiable accepted means relied upon in their home jurisdiction as a basis for sustaining such rights. INTA looks forward to specific provisions that embody the concepts for additional information requirements noted in Implementation Guidance subsection b) above.  Auditing / logging by Accreditation Authority and Identity Providers  c) The accreditation/verification activity (such as accreditation request, information on the basis of which the decision to accredit or verify identity was made) will be logged by the Accreditation Authority and Identity Providers.  d) Logged data SHALL only be disclosed, or otherwise made available for review, by the Accreditation Authority or Identity Provider, where disclosure is considered necessary to a) fulfill or meet an applicable legal obligation of the Accreditation Authority or Identity Provider; b) carry out an audit under this policy or; c) to support the reasonable functioning of SSAD and the accreditation policy.  See also auditing and logging preliminary recommendations for further details. | INTA | Support  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
|  | GBOC generally supports this recommendation and believes accreditation is necessary for an effective, efficient and legally sound SSAD.  That said, GBOC would support the addition of a “Trusted Notifier” concept as an additional layer of accreditation/verification/trust for certain Accredited Entities who are demonstrated subject matter experts who have undergone additional vetting. Upon attaining Trusted Notifier status, such requestors should be afforded special privileges in using SSAD, such as accelerated and automated disclosure responses, a presumption favoring disclosure, etc. We would be happy to work with the EPDP team to identify more specific criteria for a Trusted Notifier program as part of SSAD, and would also suggest reviewing existing registry trusted notifier systems as part of this endeavor.  In addition, any accreditation period should be as long as possible, to reduce the burden of having to frequently seek re-accreditation.  There should also be a specified and defined independent appeal mechanism for any decisions to de-accredit an accredited user on the basis of an alleged violation of the SSAD/accreditation rules. | Winterfeldt IP Group | Support  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
|  | For Requirements of the Accreditation Authority (i)3rd bullet, and (k) - add/comment: For some sets of SSAD users, to avoid the possibility of a conflict of interest, compliance with the Code of Conduct should be monitored by (and if warranted, violations addressed by) a third party independent of the Accreditation Authority. (Given the standards applied by some user groups, e.g., security professionals within the APWG, this may not be applicable, and in fact, for such group the Accreditation Authority may be ideally suited to monitor such compliance.)  For (l), "regular basis should be defined, e.g., annually.  For Accredited User Revocation & Abuse: grounds 1 and 2 should be managed by a third party, grounds 3 and 4 could be managed by the Accreditation Authority. | WIPO | Support  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
|  | We recommend a definition to specify the types of SSAD Users, such as “accredited organizations, companies, associations and individuals.” It is unclear how individuals making a request on behalf of an accredited legal entity (organization, company, association) will be validated at the time of request and then audited at a later date. We believe that Recommendation #1 should be revised to clarify whether requests made on behalf of accredited organizations must be made by individuals specifically accredited to act on behalf of that organization. Further to a), we believe that the EPDP should clarify whether SSAD will merely rely on an attestation of the individual or, preferably, rely on a Signed Assertion that the individual has the right to act on the authority of an accredited organization. It is not practically feasible for ICANN to be the sole Accreditation Authority for the myriad different types of Signed Assertions that may need to be Verified (e.g., organizations like WIPO are already better equipped to verify intellectual property rights). | InfoNetworks | Support  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
| **Significant change required: changing intent and wording** | | | |
|  | Some questions are not addressed in this recommendation:  - How will ICANN choose the identity providers? Based on which criteria?  - What will be the cost/fees of such accreditation? How will these costs/fees be determined? Who will bear those costs? | AFNIC | Concerns  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
|  | The accrediting authority role can be performed either by ICANN or by a management entity overseen by ICANN. However, If ICANN will take over operational management tasks, its role can no longer be limited to the control of registrars. For the second option which consists in designating an entity which will ensure the accreditation of SSAD users, it is essential to detail the selection process of this entity, the necessary qualifications of this entity and in which case this entity can be de-accredited. | Insance Nationale des Télécommunications de Tunis | Concerns  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
|  | “SSAD MUST only accept requests for access/disclosure from accredited organizations, companies, associations and individuals”.  The terms “companies, associations” shall be added, in order to explicitly include the participation of all types of legal person in this process. | Federation of the Swiss Watch Industry | Concerns  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
|  | As the Accreditation Authority itself will process personal data, it is recommended that it defines a privacy policy (in which it defines the purpose of the processing of personal data and the application of privacy and data protection principles and applicable laws to its operations) and when it uses outsourced services in ensuring its task the responsibility remains with the Accreditation Authority with regard to the personal data processed. Therefore it is suggested to amend point c) as follows:  c) The accreditation policy defines a single Accreditation Authority, managed by ICANN org which should include a specific privacy policy for the processing of personal data it undertakes. This Accreditation Authority MAY work with external or third-party Identity Providers that could serve as clearinghouses to Verify identity and authorization information associated with those requesting accreditation. The responsibility for the processing of personal data in this latter case shall remain with the Accreditation Authority.  As there is a growing convergence towards a set of high level principles on the protection of privacy and personal data with existing legally binding multilateral treaty, namely the sole global data protection treaty (Convention 108+), it is advisable to change point i) as follows:  i) Defines a base line “code of conduct”[2] that establishes a set of rules that contribute to the proper application of data protection laws - including the GDPR and as enshrined in international public law established by legally binding multilateral instruments - including  It is of high importance that requirements established by the accreditation policy towards accredited users are clear. For that matter it would be beneficial to refer to existing provisions and definitions of legally binding instruments  For the reason of unclarity it is suggested that point a) of the Implementation Guidance is changed as follows:  a) Recognized, applicable, and well-established organizations under the law of the Accreditation Authority could support the Accreditation Authority as an Identity Provider and/or Verify information. Proper vetting, as described in j) above, MUST take place if any such reputable and well-established organizations are to collaborate with the Accreditation Authority.  As logging data are extremely sensitive and confidential in nature, it is recommended that point d) of the Implementation Guidance is amended as follows:  d) Logged data SHALL only be disclosed, or otherwise made available for review on a case-by-case basis, by the Accreditation Authority or Identity Provider with the approval of the Accreditation Authority Auditor, where disclosure is considered necessary to a) fulfil or meet an applicable legal obligation of the Accreditation Authority or Identity Provider; b) carry out an audit under this policy or; c) to support the reasonable functioning of SSAD and the accreditation policy. | Council of Europe Data Protection Unit | Concerns  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
|  | The creation of an Accreditation Authority brings significant complications to what should be a simple transaction. An accreditation process can be beneficial for improved user tracking and to reduce the work needed by the responding Contracted Party to validate the requestor’s identity, however there are several aspects of this recommendation which should be modified and the reliance on an Accreditation Authority is misplaced.  The identity of the requestor is insufficient to demonstrate legal right to personal data; authentication of the request in combination with the identity of the requestor is what must be evaluated. Tucows does not note any circumstance in which a third party validating a requestor would circumvent either our own validation process or our review process with respect to the specific request; rather, Tucows notes multiple occasions in our experience in which a known (equivalent to accredited) requestor submitted an inappropriate request. This underscores the fact that the mere identity of the requestor is not sufficient to demonstrate any right to the requested data.  Additionally, each request for data necessitates a review of the requestor’s information and a confirmation that it remains valid and up-to-date, which is simple to bypass if a credential remains valid for ongoing reuse. | Tucows | Concerns  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |
| **Recommendation should be deleted** | | | |
|  | None. |  | Divergence  **EPDP Response:** None.  **Action Taken:** None.  [**COMPLETED**] – None. |
| **No Opinion** | | | |
|  | No comment | TUI AG, ChunKuang Wei, M3AAWG | No Opinion  **EPDP Response:** None.  **Action Taken:** None.  [**COMPLETED**] – None. |
| **No Response** | | | |
|  | General Comment:  For ease of reading and clarity in implementation, ICANN org suggests moving these definitions and the definition for “Eligible government entities” in Recommendation #2 to a separate section of the report. The rationale for this is that the definitions apply across all recommendations and are not meant to be interpreted as policy recommendations or requirements on their own.  Principles:  General Comment:  ICANN org suggests that the principles listed under Recommendation #1 move to the implementation guidance for this recommendation, as they do not seem to be intended as policy recommendations.  Bullet point d:  ICANN org suggests further clarifying principle d to specify which party is responsible for the validation of the Identity Credential, Signed Assertions, and the requested data in order to authorize the disclosure of the registration data. This is further described in the comments on bullet points f and g below.  Requirements of the Accreditation Authority:  Bullet point e:  As there are no recommendations on how the Accreditation Authority must verify the identity of the requestor, ICANN org believes it is important to understand the scale of effort the EPDP expects for the verification process. For example, how and to what type of standards would an IP attorney’s identity be validated? A cyber security researcher? If any possible SSAD user may be accredited, how would the Accreditation Authority or Identity Provider be expected to verify that an individual with the email address NAME@SLD.TLD is who they say they are? Would it be up to the Accreditation Authority or the Identity Provider to set these parameters?  Bullet point f:  This recommendation requires that “the Accreditation Authority MUST verify and manage a set of dynamic assertions/claims associated with and bound to the Identity Credential of the requestor,” but then notes that “This verification is performed by an Identity Provider.” The Accreditation Authority may not be able to verify and manage these “assertions” if a third-party Identity Provider is responsible for verifying the identity of the requestor. The Accreditation Authority may not have the necessary relationship with a requestor to verify the attributes included in a signed assertion. Can the EPDP confirm whether it is only the Identity Provider that can provide this function? If that is the case, would it be sufficient for the Accreditation Authority’s verification process to ensure a secure confirmation with the Identity Provider that the relevant “signed assertions” were provided?  Bullet point g:  As a general comment, please consider moving the recommendations related to Signed Assertions into their own recommendation, because this seems to require a series of actions and procedures that are separate from the Accreditation process. As the org understands them, Signed Assertions are meant to be additional methods for validating the identity of the requestor and attributes associated with a requestor’s identity. Can the EPDP Team confirm this assumption? Furthermore, some of the elements that must be managed and verified by the Accreditation Authority as part of the Signed Assertions seem to be related to individual requests, for example, assertion as to the purpose(s) of the request, and assertion as to the legal basis of the requestor. As Signed Assertions may then relate to individual requests rather than requests for accreditation to use the SSAD, can the EPDP further clarify why the Accreditation Authority is responsible for managing the Signed Assertions? Lastly, it would be helpful to understand if the Identity Provider is meant to generate or validate the Signed Assertions. See the comments above on bullet point f.  Bullet point h:  It is unclear how the Accreditation Authority would facilitate the validation of the Identity Credentials and Signed Assertions to “facilitate the decision of the authorization provider.” What does “facilitate” mean in this instance? Does it mean that the Accreditation Authority would share the Identity Credentials and Signed Assertions with the authorization provider (presumably the relevant Contracted Party)?  Bullet point i:  Can the team clarify its intentions in referencing GDPR standards in the context of its recommended “code of conduct” in footnote 12? Does the EPDP Team recommend that the Accreditation Authority define a baseline “code of conduct” as contemplated in Article 40 of the GDPR (with all of the associated requirements)? Or was this phrase used in a more general sense, with a reference to the GDPR as a suggested resource?  The Accreditation Authority:  Bullet point j:  The recommendation does not indicate which entity is intended to develop and enforce a “uniform baseline application procedure and accompanying requirements.” Can the EPDP confirm that it expects the Accreditation Authority to to develop a uniform baseline application procedure? Or is the expectation that the Mechanism for Evolution of the SSAD would develop this procedure?  The last sub-bullet under j) indicates that “requirements beyond the baseline” may be necessary. Is it recommended that the Accreditation Authority will have the discretion to decide when requirements beyond the baseline are necessary? Or would some other entity make this determination (e.g. the Mechanism for Evolution of the SSAD)? It is also unclear what specific procedures for validation or accreditation are contemplated and how stringent the EPDP Team envisions these procedures to be. Would it be up to ICANN org to determine what the requirements would be for accreditation? As an example, the Statement of Registrar Accreditation Policy provides criteria for the types of specific capabilities that an application for registrar accreditation must demonstrate.  De-authorization of Identity Providers:  Bullet point t:  There is no defined “authorization policy for Identity providers” in the initial report. Can the EPDP confirm that the Accreditation Authority would be expected to define this as part of its procedure for selecting and approving Identity Providers? If so, what standards would the Identity Provider have to follow? The use of SHOULD here indicates this procedure may be optional, therefore is it correct to assume that Identity Providers would still be in compliance if they chose to not include graduated penalties? Additionally, would it be correct to assume that ICANN org may choose any process and procedure to approve or reject Identity Providers?  Accredited Entities or Individuals:  Bullet point v:  Can the EPDP team clarify which entity is responsible for determining “where the accredited entity poses a demonstrable threat to the SSAD,” and when/how? As well as which entity is responsible for determining “possible limitations in SSAD’s response capacity and speed”?  Implementation guidance:  Bullet Point d:  To avoid confusion in implementation, ICANN org suggests clarifying whether this is a requirement or implementation guidance. Additionally, ICANN org suggests changing “SHALL” to “should” or removing the requirement altogether, as the statement “Logged data SHALL only be disclosed, or otherwise made available for review, by the Accreditation Authority or Identity Provider, where disclosure is considered necessary to.. support the reasonable functioning of SSAD and the Accreditation policy” may be too broad under applicable data protection law. | ICANN Org | No Response  **EPDP Response:**  **Action Taken:**  [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.] |