

Recommendation #1 – Accreditation

Please note that the staff support team has reviewed all the input received and has applied changes as follows:

- Change applied as proposed
- Change applied but with modification
- Change not applied – rationale provided
- Need further guidance from EPDP Team to decide if / what change should be applied
- Response to question posed
- Request for further input from group that provided comment

Instructions: EPDP Team members are expected to review the last column ('how addressed') and indicate if any of the changes that have been applied or have not been applied have resulted in 'cannot live' with items. Please indicate your rationale for flagging an item and provide a proposal for how your concern can be addressed factoring in previous discussions.

Group	Item # that has resulted in cannot live with status & Rationale	Proposed updated text
RrSG, IPC	29: No concerns	
BC	24: parenthetical text is too broad	"... or where they may be otherwise permitted under recommendation 1.4(d)."
RySG	8: What does it mean that "The level of verification may vary dependent on the type of applicant"? Would the level of verification be communicated to the disclosing entity? Would this also be a factor in determining if the requested data should be disclosed? Having different levels of verification hasn't been flushed out and seems problematic to add now.	Remove the text "The level of verification may vary dependent on the type of applicant" from footnote 12.

ICANN org	<p>Item #3</p> <p>1.3 e) “e) The Accreditation Authority MUST develop a specific privacy policy for the processing of personal data it undertakes as well as terms of service for its accredited users.”</p> <p>This seems to revisit language that was replaced in 1.2 c) “The Accreditation Authority MUST develop a privacy policy in accordance with the Privacy Policy for Processing of Personal Data for SSAD Users as outlined in recommendation #13.”</p> <p>Can the EPDP team please explain how these are different?</p>	<p>If the requirements are the same, suggest using the language in 1.2 c) and deleting 1.3 e). 1.2 c) can also include a reference to Terms of Use as outlined in Recommendation #13: The Accreditation Authority MUST develop a privacy policy in accordance with the Privacy Policy for Processing of Personal Data for SSAD Users and Terms of Use for SSAD Users as outlined in recommendation #13.”</p>
-----------	---	--

CANNOT LIVE WITH

Group	Text & Rationale	Proposed updated text	How Addressed
1. RySG	<p>c) . . . Overseeing MAY include monitoring for and addressing potential abuse by the party(ies) to which the function of parts thereof have been outsourced.</p> <p>Oversight must include monitoring and addressing abuse in order for oversight to be meaningful</p>	<p>c) . . . Overseeing MUST include monitoring for and addressing potential abuse by the party(ies) to which the function of parts thereof have been outsourced.</p>	<p>Change applied – EPDP Team members to flag if they cannot live with this change.</p>

2. RYSG	<p>1.5 (g) ... and thus MAY be subject to delays, and manual processing.</p> <p>This is entirely subjective and is passing opinion off as policy. Revocation will not prevent requests for disclosure, period.</p>	<p>g) For the avoidance of doubt, De-accreditation does not prevent individuals or entities from submitting future requests under the access method provisioned in Recommendation 18 of the EPDP Phase 1 Report.</p>	<p>Change applied – EPDP Team members to flag if they cannot live with this change.</p>
3. RySG	<p>We need to add a requirement that Accreditation Authorities have Terms of Service for accredited users.</p> <p>The recommendation requires that an Accreditation Authority have a Code of Conduct applicable to them (see footnote 5) but no requirement that an Accreditation Authority have Terms of Service for accredited users (even though accredited users will assert that they will adhere to any terms of service.)</p>	<p>Add to 1.1(c): The Accreditation Authority MUST develop a specific privacy policy for the processing of personal data it undertakes as well as terms of service for its accredited users.</p>	<p>Change applied – note this aligns with the requirements in the SSAD Terms and Conditions recommendation. EPDP Team members to flag if they cannot live with this change.</p>

MINOR EDITS

Group	Text & Rationale	Proposed updated text	How Addressed
4. ALAC	<p>In 1.3(b), it is unclear how one can VERIFY the assertions.</p>	<p>Replace VERIFY with RECORD, or say that the the AGREEMENT TO ASSERT will be verified.</p>	<p>Change not applied – the language says MAY verify – there may be ways in which assertions can be verified, for example by Identity Providers.</p>

5. ALAC	Authorization - A process for approving or denying disclosure non-public registration data	disclosure of non-public registration data	Change applied
6. ALAC	1.2(d) does not seem to belong in the section on accreditation. If it stays, note that the term “Central Gateway Manager” is introduced here without definition. Perhaps it is defined elsewhere in the document.	It should either be defined and used through the recommendation or replaced in 1.2(d)	Change not applied – note that Central Gateway Manager is described in section 3.1 that precedes the recommendations.
7. ALAC	Are the definitions part of Rec #1, or in a report intro?		These apply to all recommendations although many specifically apply to recommendation #1. However, definitions should be considered implementation guidance and not policy – these may be used in the development of the policy recommendations, but experience has learned that the implementation may result in tweaks to definitions that are difficult to make if these are part of the policy recommendations.
8. ALAC	1.3(a) or the footnote should note that the thoroughness of the verification may vary with the type of applicant (ie verifying that someone claims to be Microsoft will be at a different level than verifying that the e-mail address provided by a one-time user is used by that person).		Change applied – see footnote 12.
9. IPC	“For the purpose of the SSAD, the Identity Provider may be the Accreditation	“it” should be “the Accreditation Authority”	Change applied

	Authority itself or it may rely on zero or more 3rd parties. " unclear	"parties" should be "parties to perform the Identity Provider services"	
10. IPC	"Requestor – An accredited user seeking disclosure to domain name registration data through the SSAD" unclear	"to" should be "of"	Change applied
11. IPC	"1.4 Accredited User Revocation & Abuse " abuse is covered elsewhere	strike "& Abuse"	Change applied
12. IPC	"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." no normative language	"could" should be MAY	Change applied
13. IPC	"Revocation will prevent re-accreditation in the future absent special circumstances presented to the satisfaction of the Accreditation Authority." no normative language	"will" should be SHOULD	Change applied, but note that 'will' has been changed to MUST consistent with other instances where will was used.
14. IPC	"For the avoidance of doubt, De-accreditation does not prevent individuals or entities from submitting future requests under the access method provisioned in Recommendation 18 of the EPDP Phase 1 Report, but they will not be accredited, and thus MAY be subject to delays, and manual processing." capitalizing MAY is inappropriate here	"For the avoidance of doubt, De-accreditation does not prevent individuals or entities from submitting future requests under the access method provisioned in Recommendation 18 of the EPDP Phase 1 Report, but they will not be accredited, and thus may be processed manually."	Last sentence already removed as a result of input #2.

	strike "delays, and" - CPs should not be able to delay intentionally.		
15. IPC	1.7 b) "Will not be restricted in the number of SSAD" no normative language	"Will" should be "MUST"	Change applied
16. RrSG	Proposing additional text for "Signed Assertion" definition to add clarity	Add: Signed Assertions may be user-specific (e.g. to indicate professional affiliation or affirmation of lawful data handling processes) or request-specific (e.g. indicating the lawful basis for the disclosure request).	Change applied
17. RrSG	Definitions of validate/validation and verify/verification should be consolidated instead of having two definitions of the same thing		Change applied
18. RrSG	Signed assertion "Assertion as to the legal basis of the requestor" should instead be "of the request"		Change applied
19. RrSG	1.3 (c) The term "authorization provider" is only found in this one spot in this rec, and it is not defined. It must be the Rr/Ry/CGM but it's not clear.	just make it say "facilitate the decision to accept or reject"	Change applied
20. RySG	<ul style="list-style-type: none"> ● Authorization - A process for approving or denying disclosure non-public registration data. 	<ul style="list-style-type: none"> ● Authorization - A process for approving or denying disclosure of non-public registration data. 	Change applied

21. RySG	<ul style="list-style-type: none"> Requestor – An accredited user seeking disclosure to domain name registration data through the SSAD 	<ul style="list-style-type: none"> Requestor – An accredited user seeking disclosure of domain name registration data through the SSAD 	Change applied
22. RySG	<p>a. 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</p> <p>The “code of conduct” we’ve outlined in this section is applicable to the Accreditation Authority only (see Footnote 5) and not accredited users. For clarity I believe we are referring here to the safeguards or terms of service developed by the Accreditation Authority (although nowhere in this section have we required the Accreditation Authority to create terms of service, the only reference is that an accredited user will assert that they will adhere to any terms of service).</p>	<p>a. 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 any applicable safeguards or terms of service</p>	Change applied
23. RySG	<p>c) A mechanism to report an accredited user’s violation of the code of conduct</p> <p>See rational above re: code of conduct vs. terms of service</p>	<p>c) A mechanism to report an accredited user’s violation of any safeguards or terms of service</p>	Change applied

24. RySG	<p>1.7 b) Will not be restricted in the number of SSAD requests that can be submitted during a specific period of time</p> <p>For clarity, and to ensure proper safeguards for registrant / data subject rights at the core, there are instances in the recommendations that may restrict the number of requests e.g. graduated penalties etc., we cannot create a contradiction in the recommendations.</p>	<p>a. The number of SSAD requests that can be submitted during a specific period of time will not be restricted, except where the accredited entity poses a demonstrable threat to the SSAD, or where they may be otherwise permitted under these recommendations (e.g. as part of graduated penalties etc.). It is understood that possible limitations in SSAD's response capacity and speed may apply</p>	Change applied
25. ICAN N org	<p>"Identifier Credential" under the definitions also seems to be referred to as an "Identity Credential" elsewhere in the definitions (See definitions for "Validate" and "Verify"). "Identity Credential" seems to be the accurate term. Further, the definition for "Identifier Credential" also references a "unit of authentication information."</p>	<p>b. Replace "Identifier Credential" with "Identity Credential" where appropriate. Clarify what is meant by a "unit of authentication information."</p>	Change applied – changed 'unit of authentication information' to 'authenticated information'.
26. ICAN N org	<p>1.1 The EPDP Team recommends that a policy for accreditation of SSAD users is established.</p> <p>Can the EPDP team please clarify who establishes this policy? For example, is it the Accreditation Authority, in accordance with the recommendations enumerated in the remainder of Recommendation #1.</p>	<p>c. If the recommendation intends for the Accreditation Authority to establish this policy, suggested rewrite: "The EPDP Team recommends that the Accreditation Authority establish a policy for accreditation of SSAD users in accordance with the recommendations outlined in Recommendation #1."</p>	Change applied

<p>27. ICAN N org</p>	<p>1.2 The following principles underpin the accreditation policy:</p> <p>Can the EPDP team please clarify if the bullets listed under 1.2 are requirements that form the accreditation policy referenced in 1.1?</p>	<p>If the “principles” are intended to be recommendations to form the accreditation policy, suggest rewriting as: “1.2 The following recommendations MUST be included in the accreditation policy:”</p> <p>d.</p>	<p>Change applied</p>
<p>28. ICAN N org</p>	<p>1.2.(c) The Accreditation Authority MUST develop a specific privacy policy for the processing of personal data it undertakes.</p> <p>Can the EPDP team please clarify what it means by "a specific privacy policy?"</p> <p>Is this referencing the privacy policy found in the combined Rec 13, paragraph a) Privacy Policy for Processing of Personal Data for SSAD Users?</p>	<p>If the answer to the clarifying question is, suggest rewriting as: “The Accreditation Authority MUST develop a privacy policy in accordance with the Privacy Policy for Processing of Personal Data for SSAD Users as outlined in Rec. 13.”</p>	<p>Change applied</p>
<p>29. ICAN N org</p>	<p>1.7.(a) seems redundant with the policies outlined in the combined Rec. 10-13-14, which cover Terms of Use, Disclosure Agreement and Acceptable Use. Would the EPDP team consider referencing those recommendations instead to provide greater clarity during implementation?</p>		<p>EPDP Team to confirm whether there are any concerns about removing the requirements in this section but instead refer to recommendations 10-13-14 that cover terms of use, disclosure agreement and acceptable use.</p>

30. ICAN N org	1.9 seems redundant with Rec #15.	Suggest deleting paragraph 1.9.	Change applied
-------------------	-----------------------------------	---------------------------------	----------------