Recommendation #1 – Accreditation

The staff support team has reviewed the Rec. 1 feedback provided by the deadline and is putting forward the following topics / issues for discussion during Thursday's meeting. The input on these topics / issues will be used to develop a next iteration of the recommendation text for EPDP Team review. Note: known concerns, which have been considered and discussed previously, have not been included and will not be discussed again unless new information has been provided. If EPDP Team Members believe new information has been provided during the public comment period, they are expected to flag this within the discussion table.

Signed Assertions:

Based on the input provided, it is our understanding that:

- An Identifier Credential is static and typically does not change, while Signed Assertions are dynamic and may change based on the request (purpose, legal basis, type, urgency, etc.).
- Signed assertions are only used to associate/bind attributes to an identity. These attributes are dynamic per request, but can be vetted and managed up front as needed - during the Accreditation Process.
- An Accreditation Authority can establish various assertions for a specific Identifier Credential up front or dynamically create them on a per request basis. How this is determined is an implementation detail.
- The Accreditation Authority may store multiple Signed Assertions per Identifier Credential, but the Requestor must invoke the relevant assertions per request. (In other words, it is not the objective to attach as many signed assertions as possible and hope that one sticks).
- If ICANN Org as the Accreditation Authority decides to engage a 3rd party Identity Provider, the 3rd Party Identity Provider should be able to issue/manage both Identity Credentials and Signed Assertions.
- The policy recommendation may include examples of what signed assertions may be, but these are expected to be further worked out in the implementation phase.

Questions / clarifications Signed Assertions:

1. Are there any further elements or aspects that require clarification? If not, can the Staff Support Team proceed to rewrite this section of the recommendation for EPDP Team review?

Trusted Notifiers:

Questions/clarifications:

2. Please describe the benefits or purpose to either the notifier, the relevant contracted party or the Central Gateway Operator.

3. Is this a concept that fits in the accreditation recommendation or instead, is this a concept that may develop over time, based on trust gained, that could result in a specific disclosing controller / Contracted Party assigning such a status to an accredited entity that could result in specific privileges (for example, a request from a CP to automate all disclosure requests from such a trusted notifier)? If this is a concept that may develop over time, is this something that could be described as an example of how SSAD may evolve as trust is gained and risk assessed over time?

Accreditation Authority

For clarity:

- The Accreditation Authority is responsible for the verification, issuance and ongoing management of both the Identity Credential and the Signed Assertions.
- The Accreditation Authority MAY outsource this to a 3rd party as needed (e.g., WIPO, M3AAWG, etc.).
- The entity responsible for the validation of the Identity Credential and Signed Assertions and the request as a whole is the Central Gateway - upon receipt of a request from a Requestor. What the Central Gateway relays to the Contracted Party should be left to implementation (e.g., full request or parsed and sent into a different format).
- The flow of requests through the system is always Requestor --> Central Gateway manager --> Registrar/Registry.
- The list of user types is illustrative rather than determinative and does not indicate who will actually end up using the SSAD.
- Each individual-person SSAD requestor should have their own accreditation (with their own distinct login credential), while any user who is acting on behalf of an organization (such as their employer or an association they represent) should have their login tied to that organization's accreditation.

Questions/clarifications:

4. Are there any further elements or aspects that require clarification or on the basis of the above the Staff Support Team can go ahead and rewrite this section of the recommendation for EPDP Team review, making clear that certain aspects are expected to be further worked out during implementation?
5. In which circumstances would requests flow to the registry? Are these circumstances at the discretion of the Central Gateway manager, for example, in case a registrar has gone out of business and all its names are in the process of being transferred to a different registrar? As a reminder, the EPDP Team has included the following footnote in its report: "8 As a default, the Central Gateway Manager will send disclosure requests to Registrars, but that does not preclude the Central Gateway Manager from sending disclosure request so Registries in certain circumstances. The EPDP Team will further consider what these circumstances could be."

Re-accreditation

Note that the re-accreditation period is expected to be established during the implementation phase, but it would be helpful if the EPDP Team includes a clarification of what it considers a reasonable timeframe. The Staff Support Team had suggested to include a reference to the registrar accreditation period, which is currently 5 years, but some commenters have expressed been expressed.

6. What would be a reasonable time period to provide as a possible reference? The concerns expressed seemed to relate to what happens if things change in the 5 year period – could this be addressed by making clear that if there would be any changes in the accredited entities' situation, there would be an obligation for the accredited entity to notify the Accreditation Authority so that its accreditation could be reviewed and updated accordingly? This, for example, could be done through an annual (?) reminder in which the accredited entity is requested to review and reconfirm or update information associated with their accreditation?

Requirements for the Accreditation Authority

Based on the input and clarifications provided, the Staff Support Team will add further detail to the recommendation, including clarifying aspects that are expected to be defined in the implementation phase.

7. Are there any further elements or aspects that may require clarification?

Revocation Policy

Add that there should be an appeals mechanism for any decisions to de-accredit an accredited entity on the basis of an alleged violation of the system, but with the understanding that an accreditation remains suspended while the appeal is ongoing, and the decision process must be transparent.

8. Any concerns about adding this requirement?

Code of conduct reference

There seems to be agreement that this section needs clarification, but no guidance has been provided on how this should be clarified. This is the current language included in the Initial Report:

"The Accreditation Authority - q) Defines a base line "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 Mechanism that allow 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. "

[12] To see how this is defined in the context of GDPR, see https://edpb.europa.eu/sites/edpb/files/consultation/edpb-20190219_guidelines_coc_public_consultation_version_en.pdf.

9. What clarification needs to be provided to make clear what is meant with the reference to 'code of conduct'?

Baseline application procedure and accompanying requirements for all applicants

Based on the input provided, it is our understanding that it is the expectation that:

- The definition of eligibility requirements will be reviewed and revised over time with the learnings from the accreditation process.
- There should be a clear timeline for the accreditation process and response.
- The Accreditation Authority will be responsible for developing the accreditation application procedure and accompanying requirements, in alignment with the policy recommendations and implementation guidance provided in the Final Report.

10. Are there any further elements or aspects that may require clarification?

Auditing of Accreditation Authority

Discuss frequency of auditing under auditing recommendation.

Reporting by Accreditation Authority

Consider this in context of new reporting recommendation that is out for EPDP Team review.

Accredited User Revocation & Abuse

The accreditation authority may obtain information from other parties in making a determination that abuse has taken place, but this is an implementation detail, not a policy determination.

Sanctions will be further determined and developed in the implementation phase, on the proposal of ICANN org.

11. Are there any further elements or aspects that may require clarification?

Definition of abuse (revocation and accredited entity requirements)

12. How should abuse of the system be defined and differentiated (if applicable) from violation of the code of conduct? Should the definition of abuse be considered in conjunction with Rec. 12?
13. What further guidance can be provided in relation to ‘prevent abuse of data received’ by the accredited entity or individual (see u)?
14. “Demonstrable threat to the SSAD” (see v) – is that something that can be left to implementation based on SLAs and possible input through the mechanism?

Abuse by Accreditation Authority

15. There is agreement that the Accreditation Authority should also be supervised for potential abuse and the proposed suggestion is that ICANN Org should be identified as the supervisor of accreditation authorities, but ICANN org IS the Accreditation Authority. Was this intended to indicate that if ICANN org outsources part or all of the Accreditation Authority functionalities, it is responsible for overseeing and addressing potential abuse?

De-authorization of Identity Providers

An appeals mechanism should be available for Identity Providers.
As the use of Identity Providers is optional, the Accreditation Authority is expected to develop an authentication policy for Identity Providers, if it decides to use Identity Providers, factoring in the policy recommendations and implementation guidance provided in the Final Report as well as any further guidance the IRT may provide in the implementation phase.

16. Are there any further elements or aspects that may require clarification?

Implementation guidance

Indicate that further details in relation to ‘information asserting trademark ownership’ as well as ‘recognized, applicable and well-established organizations’ will be further developed in the implementation phase.