Building Block f) *(Authentication / authorization / accreditation[1])*

Staff support team comment:

Also need to address charter question a7) How can RDAP, that is technically capable, allow Registries/Registrars to accept accreditation tokens and purpose for the query? Once accreditation models are developed by the appropriate accreditors and approved by the relevant legal authorities, how can we ensure that RDAP is technically capable and is ready to accept, log and respond to the accredited requestor's token? EPDP Team to consider reviewing Sections 5 and 6 in TSG01, which discusses technical requirements for credentials in RDAP.

Further details would need to be provided about what the benefits of accreditation are.

Re. "EDPB for review" - Need to confirm what happens after this review – is it ICANN Org who then modifies the implementation of the policy to add the accreditation mechanism and related requirements?

Re. "revocation" - Need further details on what revocation would mean in practice e.g. no further access to SSAD?

The EPDP Team recommends that user groups interested in accreditation should self-organize and develop a proposed accreditation mechanism that is shared with the European Data Protection Board for review. Any such accreditation mechanism is expected to adhere to the following principles:

a) Must provide for a mechanism for de-accreditation in case of abuse of access / disclosure of non-public registration data;
b) Accreditation may not result in any kind of automatic access / disclosure, but it is expected to facilitate review of requests and automation, where applicable;
c) [Other]

Those wanting to be accredited must:

a) Agree to only use the data for the legitimate and lawful purpose described above;
b) If applicable, only issue disclosure requests with respect to the trademark(s) where ownership is evidenced;
c) Agree to:
    - the terms of service, in which the lawful use of data described;
    - prevent abuse of data received;
    - be subject to de-accreditation if they are found to abuse use of data;
    - maintain a register of all requests also including the respective rightsholders name (subject to audits).

[1] Charter questions b1, b2 and b3

Failure to abide by safeguards would affect accreditation, including the possibility of revocation.

Comments / concerns / questions to be considered in relation to building block f):

- *Is accreditation necessary?*
- *Consider equating "Accreditation" Certification under art 42/43 of the GDPR. Is there any other form of 'accreditation' that could provide anything other than verification of identity? Accreditation may be an additional layer on top of certification, specifically aimed at disclosure requests in the SSAD: it would be up to the SSAD provide to undergo a meaningful assessment of that accreditation/certification before it is deemed acceptable. If this is approach is followed, another building block would need to be added: "review and acceptance of 'accreditation' standards".*
- *Consider whether this is the beginning of a list of enforcement considerations should or in addition to GDPR compliance (where applicable) basic entry requirements for a 3rd part accreditation to be deemed as an acceptable certification for SSAD purposes? In the latter case it would not be a requirement for "those wanting to be accredited" but a requirement on the "accrediting entity" to demonstrate and prove how they can enforce this.*
- *Consider that revocation would not be a responsibility of SSAD but of the 'accreditation body' but the SSAD must have a way of ensuring that such a body is auditing / and enforcing requirements. Limiting or removing accreditation is the ONLY mechanism to enforce the data protection requirements of the SSAD but consider adding further details on who / how this would happen and be verified.*
- *Re. bullet 4, clarify why this is required or consider deleting it.*