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

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;

[1] Charter questions b1, b2 and b3

- maintain a register of all requests also including the respective rightsholders name (subject to audits).

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.*

Building block j - *(Authentication / authorization / accreditation[2])*
(Entity disclosing the data)

Staff support team comment:
Also needs 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?

"re. Accreditation authority – needs a definition / description.

The EPDP Team recommends that the entity disclosing the data must:

a) Provide the ability for confirmed accreditors to confirm accredited requestors in SSAD;

[2] Charter questions b1, b2 and b3

b) Provide for a mechanism to report abuse by an accredited user which is relayed to the accreditation authority for handling;
c) Confirm the validity of each request;
d) [Other]

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

- *Consider addressing issue of accreditation first.*
- *Re. a), consider clarifying further.*
- *Re. b) is there a conflict of interest in having these reports relayed to the accreditation authority? How can independent review be assured?*
- *Re. c) what is meant with 'validity'? Is this word too loaded? Does it mean to validate the credential issued to the requestor by the Accreditation body?*

From SSAD Worksheet:

Authentication / authorization / accreditation of user groups

Objective:

- Establish if authentication, authorization and/or accreditation of user groups should be required
    - Can an accreditation model compliment or be used with what is implemented from EPDP-Phase 1 Recommendation #18?
- If so, establish policy principles for authentication, authorization and/or accreditation, including addressing questions such as:
    - whether or not an authenticated user requesting access to non-public WHOIS data must provide its legitimate interest for each individual query/request.
- If not, explain why not and what implications this might have on queries from certain user groups, if any.

Related mind map questions:

P1-Charter-a/b

(a) Purposes for Accessing Data - What are the unanswered policy questions that will guide implementation?
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?

(b) Credentialing – What are the unanswered policy questions that will guide implementation?
b1) How will credentials be granted and managed?
b2) Who is responsible for providing credentials?
b3) How will these credentials be integrated into registrars'/registries' technical systems?

Annex to the Temporary Specification

1. Pursuant to Section 4.4, continuing community work to develop an accreditation and access model that complies with GDPR, while recognizing the need to obtain additional guidance from Article 29 Working Party/European Data Protection Board.

TSG-Final-Q#2

Identify and select Identity Providers (if that choice is made) that can grant credentials for use in the system.

Materials to review:

Description	Link	Required because
Identification and authentication in the TSG model	https://www.icann.org/en/system/files/files/technical-model-access-non-public-registration-data-30apr19-en.pdf page 23-24	
EWG Final Report - RDS Contact Use Authorization and RDS User Accreditation Principles	https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf page 39-40 and page 62-67	
Draft Framework for a Possible Unified Access Model for Continued Access to Full WHOIS Data - How would authentication requirements for legitimate users be developed?	https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-20aug18-en.pdf pages 9-10, 10-11, 18, 23	

Related EPDP Phase 1 Implementation:
None expected.

Tasks:

- Review materials listed above and discuss perspectives on authentication / authorization.(EPDP)
- Confirm definitions of key terms Authorization, Accreditation and Authentication
- Determine full list of policy questions and deliberate each
- Determine possible solutions or proposed recommendation, if any
- Confirm all charter questions have been addressed and documented