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.
g) and h) EPDP Team to provide clarity on what "regular basis" entails.

EPDP Team to consider whether same framework applies to LE or whether a separate framework or additional provisions are needed to address LE accreditation.

The EPDP Team recommends that a framework for accreditation of SSAD users is established. Such an accreditation framework should adhere to below draft principles:

a) Accredited entities may be legal persons or individuals;
b) The accreditation authority MUST have a uniform baseline application procedure and accompanying requirements for those requesting accreditation, noting, however, there may be instances when an applicant may be required to provide additional documentation (for example, an intellectual property owner may be required to provide documentation of a valid trademark);
c) The accreditation framework should [RRSG COMMENT: Change 'should' to 'MUST'] be focused on confirming the identity of the requestor and related aspects that would facilitate the authentication of an SSAD request, for example, any relevant trademarks a requestor may hold. Accreditation must [RRSG COMMENT: Change 'must' to 'MUST'] not result in automatic access / disclosure, but it is expected to facilitate or automate the review of requests, where applicable;
d) The accreditation authority MUST provide for a mechanism for de-accreditation in case of system abuse;
e) The accreditation framework preferably has one ICANN-approved accreditation authority responsible for accreditation, but the ICANN-approved accreditation authority may work with other entities that could serve as clearinghouses and/or verify information that is provided by those requesting accreditation;
f) The SSAD MUST accommodate requests for access/disclosure from non-accredited organizations or individuals, irrespective of the ultimate accreditation framework; [RRSG COMMENT: If non-accredited users can make requests for non-public data via the SSAD, what is the purpose of accreditation? Accreditation should be required for all users (individuals or organizations), as part of the process to confirm their lawful basis for data disclosure. If the Rr/Ry has a process to take direct requests (as required under Rec 18 from Phase 1 Final Report) there would be no need for non-accredited entities to request data via SSAD.]

[1] Charter questions b1, b2 and b3

g) The accrediting authority MUST be audited by an independent auditor on a regular basis. 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 case of repeated failure, a new accreditation authority must be identified or created;
h) Accreditation must be a paid-for service. Accredited users must be offered lower fees for submission of SSAD requests, as the administrative burden of authenticating SSAD requests will likely be significantly reduced; [RRSG COMMENT: We support the suggestion to move this to the Financial Sustainability building block. We will have further comments when this point is addressed in that context.]
i) The accreditation framework must be focused on organizations that are expected to submit regular SSAD requests;
j) SSAD must provide the ability for the accreditation authority to confirm accredited requestors in SSAD;
k) SSAD must provide for a mechanism to report abuse by an accredited user which is relayed to the accreditation authority for handling.

Implementation Guidance

In relation to accreditation, the EPDP Team provides the following implementation guidance:

a) Reputable and well-established organizations such as WIPO, for example, could support the accreditation authority as a clearinghouse and/or verify information. [RRSG COMMENT: "Reputable" is a vague term; this description should be replaced with "Recognized, applicable, and well-established organizations". Specific organizations should not be called out here; otherwise, work should be done to identify all such organizations, so the phrase "such as WIPO, for example" should be removed entirely.] Proper vetting must take place if any such reputable and well-established organizations are to collaborate with the accreditation authority.

Accredited organizations [RRSG COMMENT: Accreditation is available to Individuals and Organizations (see above), so these requirements should not be specific to Organizations only. Suggest change to to "Accredited Users".]:

b) Those accredited must agree to:
    - only use the data for the legitimate and lawful purpose stated;
    - the terms of service, in which the lawful uses of data are described;
    - prevent abuse of data received;
    - [RRSG COMMENT: Add 'cooperate with any audit or information requests as a component of an audit;']
    - be subject to de-accreditation if they are found to abuse use of data or accreditation policy / requirements;
c) Will not be restricted in the number of SSAD requests that can be submitted at a time, except where the accredited organization poses a demonstrable threat to the SSAD. [RRSG Comment: Operationally, there must be some reasonable and practical limits on how many requests can be submitted, either during a single session or over a given time period. See: Access Policy.]

De-accreditation:

d) The de-accreditation policy should include graduated penalties. In other words, not every violation of the system will result in de-accreditation; however, de-accreditation may occur if the accredited organization continues to violate the policy.
e) De-accreditation will occur when the accreditation authority determines that the accredited organization has materially breached the conditions of its accreditation based on; a) a third-party complaint received; b) results of an audit or investigation by the accreditation authority or independent auditor; or c) any misuse or abuse of privileges afforded.
f) De-accreditation will prevent re-accreditation in the future absent special circumstances presented to the satisfaction of the accreditation authority.
g) De-accreditation does not prevent the organization from submitting an SSAD request as an unaccredited organization.

Fees: [RRSG COMMENT: This section should also be moved to the Financial Sustainability building block.]

h) Accreditation applicants must pay a to-be-determined non-refundable fee proportional to the cost of validating an application.
i) Rejected applicants may re-apply, but the new application(s) will be subject to the application fee.
j) Fees are to be established by the accreditation authority.
k) Accredited organizations must renew their accreditation annually.

Auditing / logging [RRSG COMMENT - Need some additional work here. Who conducts the audit? How often? We need accredited users to agree (in advance) to comply with auditor requests. Also, what exactly is included in the logs? "Query activity" is vague and could include a variety of things]

l) The query activity of all accredited organizations will be logged by the SSAD.
m) Logged data will remain confidential by default and will only be revealed under legal justifications. [RRSG COMMENT: Add to (m) Logged data will be retained in accordance with applicable law]
n) In the event of an audit or claim of misuse, logs may be requested for examination by the accreditation authority or the independent auditor.

[If there is support for the framework developed by Alex/Milton, this could be included here?]

The EPDP Team applied the following definitions in this context:

- **Accreditation** - An administrative action by which a designated authority declares that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards.[2]

[2] RFC 4949 - "Internet Security Glossary, Version 2", p. 13

- **Accreditor** - A management official [or entity] who has been designated to have the formal authority to "accredit" an information system, i.e., to authorize the operation of, and the processing of sensitive data in, the system and to accept the residual risk associated with the system.[3]
- **Authentication** - The process of verifying a claim that a system entity or system resource has a certain attribute value.
    - An authentication process consists of two basic steps:
        - Identification step: Presenting the claimed attribute value (e.g., a user identifier) to the authentication subsystem.
        - Verification step: Presenting or generating authentication information (e.g., a value signed with a private key) that acts as evidence to prove the binding between the attribute and that for which it is claimed. (See: verification.)[4]
- **Authorization** - A process for granting approval to a system entity to access a system resource.[5] [For the SSAD the resource is non-public registration data.]
- **Credential**
    - "**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 verifying an identity claimed by an entity that attempts to access a system. Example: [Username/Password], [OpenID credential], X.509 public-key certificate.
    - "**authorization credential**": A data object that is a portable representation of the association between an identifier and one or more access authorizations, and that can be presented for use in verifying those authorizations for an entity that attempts such access. Example: [OAuth credential], X.509 attribute certificate.[6]
- **De-accreditation -** An administrative action by which a designated authority declares that an information system is no longer approved to operate in a particular security configuration with a prescribed set of safeguards.[7]
- **Identification** - An act or process that presents an identifier to a system so that the system can recognize a system entity and distinguish it from other entities.[8]
- **Identifier** - A data object that definitively represents a specific identity of a system entity, distinguishing that identity from all others.[9]
- **Identity Provider -** Responsible for verifying the identity of a requestor and managing an identifier credential (issue, validate, revoke) associated with the requestor. NOTE: The Identity Provider may be associated with an Accreditation Body or be a separate function.[10]

---

[3] RFC 4949 - "Internet Security Glossary, Version 2", p. 14
[4] RFC 4949 - "Internet Security Glossary, Version 2", pp. 26-27
[5] RFC 4949 - "Internet Security Glossary, Version 2", p. 29
[6] RFC 4949 - "Internet Security Glossary, Version 2", p. 84
[7] Definition suggested by Alex.
[8] RFC 4949 - "Internet Security Glossary, Version 2", p. 145
[9] RFC 4949 - "Internet Security Glossary, Version 2", p. 146
[10] Definition suggested by Alex.

- **Revocation** - The event that occurs when an Identity Provider declares that a previously valid credential has become invalid.[11]

[11] Definition suggested by Alex.

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