Please note:
Text in green is text from the Initial Report that has not been changed.
Text in black and highlighted in yellow are updates that have been made in response to input provided on the discussion table and subsequent discussion during the EPDP Plenary session on 9/4 reviewing the discussion items identified.
Text in black may change as a result of outstanding discussion items that are to be reviewed during the 16/4 plenary session.
Text highlighted in blue has been integrated from recommendation #2 or added in order to consolidate where possible recommendation #1 and #2.

Definitions

- **Accreditation** - An administrative action by which the accreditation authority declares that a user is ~~approved~~ **eligible** to **use** ~~gain access to~~ SSAD in a particular security configuration with a prescribed set of safeguards.
- **Accreditation Authority** - A management entity who has been designated to have the formal authority to "accredit" users of SSAD, i.e., to confirm and Verify the identity of the user (represented by an Identifier Credential) and assertions (or claims) associated with the Identity Credential (represented by Signed Assertions).
- **Accreditation Authority Auditor** – The entity responsible for carrying out the auditing requirements of the Accreditation Authority, as outlined in Preliminary Recommendation #18. The entity could be an independent body or, if ICANN Org ultimately outsources the role of Accreditation Authority to a third party, ICANN Org MAY be the Accreditation Authority Auditor.
- **Authentication** - The process or action of Validating the Identity Credential and Signed Assertions of a Requestor.
- **Authorization** - A process for approving or denying disclosure non-public registration data.
- **De-accreditation of Accreditation Authority –** An administrative action by which ICANN org revokes the agreement with the accreditation authority, if this function is outsourced to a third party, following which it is no longer approved to operate as the accreditation authority.
- **Eligible government entity**: an entity that is considered by its government (including local government) to require access to RDDS data for the exercise of a public policy task.

Clarifying questions for the GAC Team:

1. *Is it possible to define 'public policy' or further narrow the description by, for example, referring to 'law enforcement tasks'? Concerns are expressed in the public comments that public policy is too broad to warrant a special accreditation status. Some have also suggested clarifying whether this applies to governmental bodies at all levels.*

- **"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 Validating an identity claimed by an entity that attempts to access a system. Example: Username/Password, OpenID credential, X.509 public-key certificate.
- **Identity Provider -** Responsible for 1) Verifying the identity of a requestor and managing an Identifier Credential associated with the requestor and 2) Verifying and managing Signed Assertions associated with the Identifier Credential. For the purpose of the SSAD, the Identity Provider may be the Accreditation Authority itself or it may rely on zero or more 3rd parties.
- **Requestor – An accredited user seeking disclosure to non-public domain name registration data through the SSAD**
- **Revocation of User Credentials-** The event that occurs when an Identity Provider declares that a previously valid credential has become invalid.
- **"Signed Assertion"**: A data object that is a portable representation of the association between an Identifier Credential and one or more access assertions, and that can be presented for use in Validating those assertions for an entity that attempts such access. Example: [OAuth credential], X.509 attribute certificate.
- **Validate -** To test or prove the soundness or correctness of a construct. (Example: The Discloser will Validate the Identity Credential and Signed Assertions as part of its Authorization process.)
- **Validation -** Establish the soundness or correctness of a construct.
- **Verify -** To test or prove the truth or accuracy of a fact or value. (Example: Identity Providers Verify the identity of the requestor prior to issuing an Identity Credential.)
- **Verification -** The process of examining information to establish the truth of a claimed fact or value.

RECOMMENDATION 1: Accreditation[1]

1.1 The EPDP Team recommends that a policy for accreditation of SSAD users is established. Specific provisions apply for the accreditation of governmental entities, where indicated below.

1.2 The following principles underpin the accreditation policy:

a) SSAD MUST only accept requests for access/disclosure from accredited organizations or individuals. However, accreditation requirements MUST accommodate any intended user of the system, including an individual or organization who makes a single request. The accreditation requirements for regular users of the system and a one-time user of the system MAY differ.

[1] Note that accreditation is not referring to accreditation/certification as discussed in GDPR Article 42/43.

b) Both legal persons and/or individuals are eligible for accreditation. An individual accessing SSAD using the credentials of an accredited entity (e.g. legal persons) warrants that the individual is acting on the authority of the accredited entity.[2]
c) The accreditation policy defines a single Accreditation Authority, managed by ICANN org, **which is responsible for the verification, issuance and ongoing management of both the Identity Credential and the Signed Assertions**. **The Accreditation Authority MUST develop a specific privacy policy for the processing of personal data it undertakes.** This Accreditation Authority MAY work with external or third-party Identity Providers that could serve as clearinghouses to Verify identity and authorization information associated with those requesting accreditation. **The responsibility for the processing of personal data in this latter case shall remain with the Accreditation Authority.**
d) The decision to authorize disclosure of registration data, based on validation of the Identity Credential, Signed Assertions, and data as required in preliminary recommendation concerning criteria and content of requests, will reside with the Registrar, Registry or the Central Gateway Manager, as applicable.
e) SSAD SHOULD ensure reasonable access to RDDS for entities that require access to this data for the exercise of their public policy task. In view of their obligations under applicable data protection rules, the final responsibility for granting access to RDDS data will remain with the party that is considered as the controller for the processing of that RDDS data that constitutes personal data. Notwithstanding these obligations, the decisions that these data controllers will need to make before granting access to RDDS data to a particular entity, can be greatly facilitated by means of the development and implementation of an accreditation procedure. The accreditation procedure can provide data controllers with information necessary to allow them to assess and decide about the disclosure of data.
f) Accreditation does not guarantee disclosure of the data. The final responsibility for the decision to disclose data lies with the data controller.

1.3 Requirements of the Accreditation Authority

a) Verify the Identity of the Requestor: The Accreditation Authority MUST verify the identity of the requestor, resulting in an Identity Credential.[3]
b) Management of Signed Assertions: The Accreditation Authority MUST verify and manage a set of dynamic assertions/claims associated with and bound to the Identity Credential of the requestor. This verification, **which may be** performed by an Identity Provider, results in Signed Assertion. Signed Assertions[4] convey information such as:

[2] Implementation guidance: The accredited entity is expected to develop appropriate policies and procedures to ensure appropriate use by an individual of its credentials. **Each user must be accredited, but a user acting on behalf of an organization, must have their accreditation tied to its organization's accreditation.**

[3] **Implementation guidance: ICANN org should use its experience in other areas where verification is involved, such as registrar accreditation, to put forward a proposal for verification of the identity of the requestor during the implementation phase.**

[4] **For clarity, Signed Assertions are dynamic and may change based on the request (purpose, legal basis, type, urgency, etc.) compared to an Identifier Credential, which is static and typically does not change. Signed assertions are only used to**

- Assertion as to the purpose(s) of the request
- Assertion as to the legal basis of the requestor
- Assertion that the user identified by the Identity Credential is affiliated with the relevant organization
- Assertion regarding compliance with laws (e.g., storage, protection and retention/disposal of data)
- Assertion regarding agreement to use the disclosed data for the legitimate and lawful purposes stated
- Assertion regarding adherence to safeguards and/or terms of service and to be subject to revocation if they are found to be in violation
- Assertions regarding prevention of abuse, auditing requirements, dispute resolution and complaints process, etc.
- Assertions specific to the requestor – trademark ownership/registration for example
- Power of Attorney statements, when/if applicable.

c) Validation of Identity Credentials and Signed Assertion**s**, in addition to the information contained in the request, facilitate the decision of the authorization provider to accept or reject the Authorization of an SSAD request. For the avoidance of doubt, the presence of these credentials alone DOES NOT result in or mandate an automatic access / disclosure authorization. However, the ability to automate access/disclosure authorization decision making is possible under certain circumstances where lawful.

d) Define a base line "code of conduct"[5] that establishes a set of rules that contribute to the proper application of data protection laws - including the GDPR, including:
   - A clear and concise explanatory statement.
   - A defined scope that determines the processing operations covered (the focus for SSAD would be on the Disclosure operation.)
   - Mechanism that allow for the monitoring of compliance with the provisions.
   - 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.
   - Description as to the extent a "consultation" with stakeholders has been carried out.

associate/bind attributes to an identity. These attributes are dynamic per request, but can be vetted and managed up front as part of the Accreditation Process as needed. The 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 to be further worked out in the implementation phase. The Accreditation Authority may store multiple Signed Assertions per Identifier Credential, but the Requestor must invoke the relevant assertions per request. It should not be the objective to attach as many signed assertions as possible to a request.

[5] ~~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.~~ For the avoidance of doubt, the code of conduct referenced here is not intended to refer to **the Code of Conduct as described in the GDPR.**

e) Develop a baseline application procedure: The Accreditation Authority MUST ~~have~~ **develop** a uniform baseline application procedure and accompanying requirements for all applicants, including governmental entities,[6] requesting accreditation,[7] including:
    i. Accreditation timeline
    ii. Definition of eligibility requirements for accredited users
    iii. Identity Validation, Procedures
    iv. Identity Credential Management Policies: lifetime/expiration, renewal frequency, security properties (password or key policies/strength), etc.
    v. Identity Credential Revocation Procedures: circumstances for revocation, revocation mechanism(s), etc. [see also "Accredited User Revocation & abuse section below]
    vi. Signed Assertions Management: lifetime/expiration, renewal frequency, etc.
    vii. NOTE: requirements beyond the baseline listed above may be necessary for certain classes of requestors.

f) Define dispute resolution and complaints process: The Accreditation Authority MUST define a dispute resolution and complaints process to challenge actions taken by the Accreditation Authority. The defined process MUST include due process checks and balances.

g) Audits: The Accreditation Authority MUST be audited by an 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 cases of repeated failure, a new Accreditation Authority must be identified or created. Additionally, accredited entities MUST be audited for compliance with the accreditation policy and requirements on a regular basis; (Note: detailed information regarding auditing requirements can be found in the Auditing preliminary recommendation).

h) User Groups: The Accreditation Authority MAY develop user groups / categories to facilitate the accreditation process as all requestors will need to be accredited, and accreditation will include identity verification.

i) Reporting: The Accreditation Authority MUST report publicly and on a regular basis on the number of accreditation requests received, accreditation requests approved/renewed, accreditations denied, accreditations revoked, complaints received and information about the identity providers it is working with. **See also recommendation #[NEW] on reporting**.

j) Renewal: The Accreditation Authority MUST establish a timeline and requirements for the renewal of the accreditation.[8]

k) Confirmation of user data: The Accreditation Authority MUST send periodic reminders (e.g., yearly) to accredited users to confirm user data and remind accredited users to

[6] For the avoidance of doubt, the accreditation authority for governmental entities may not be the same entity as the accreditation authority for non-governmental entities. [GAC colleagues: please edit/clarify as you see fit.]

[7] Implementation guidance: it is the expectation that the uniform baseline application procedure and accompanying requirements will be reviewed and revised over time, factoring in lessons learned. Input may also be provided by the mechanism for the evolution of SSAD – see recommendation #19.

[8] Implementation guidance: as a best practice, the re-accreditation period and requirements for Registrars may be considered, which is currently 5 years. For the avoidance of doubt, nothing prohibits the Accreditation Authority from requiring additional documentation upon accreditation renewal.

keep the information required for accreditation up to date. Changes to this required information MAY result in the need to re-accredit.

1.4 Accredited User Revocation & Abuse

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.[9] A non-exhaustive list of examples where revocation may apply include 1) the accredited user's violation of the code of conduct, 2) the accredited user's abuse of the system, 3) a change in affiliation of the accredited user, or 4) where prerequisites for accreditation no longer exist.

b) The Accreditation Authority MUST make available an appeals mechanism to allow an accredited user to challenge the decision to revoke the accredited user's status. However, for the duration of the appeal, the accredited user's status will remain suspended. Outcomes of an appeal MUST be reported in a transparent manner.

c) A mechanism to report abuse committed by an accredited user MUST be provided by SSAD. Reports MUST be relayed to the Accreditation Authority for handling. **The Accreditation Authority MAY also obtain information from other parties in making a determination that abuse has taken place.**

d) The revocation policy for individuals/entities SHOULD include graduated penalties; **the penalties will be further detailed during implementation, factoring in how graduated penalties are applied in other ICANN areas**. In other words, not every violation of the system will result in Revocation; however, Revocation MAY occur if the Accreditation Authority determines that the accredited individual or entity has materially breached the conditions of its accreditation and failed to cure based on: i) a third-party verified complaint received; ii) results of an audit or investigation by the Accreditation Authority or auditor; iii) any misuse or abuse of privileges afforded; iv) repeated violations of the accreditation policy; v) results of audit or investigation by a DPA.

e) 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.

f) Revocation will prevent re-accreditation in the future absent special circumstances presented to the satisfaction of the Accreditation Authority.

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, but they will not be accredited, and thus MAY be subject to delays, and manual processing.

1.6 De-authorization of Identity Providers

a) The authorization policy for Identity providers SHOULD include graduated penalties. In other words, not every violation of the policy will result in De-authorization; however,

[9] For clarity, a legal entity would not be automatically de-accredited for the single action of an individual user whose accreditation is linked to the accreditation of the legal entity, but the entity may be held responsible for the actions of the individual user whose accreditation is linked to that of the legal entity.

De-authorization may occur if it has been determined that the Identity Provider has materially breached the conditions of its contract and failed to cure based on: i) a third-party complaint received; ii) results of an audit or investigation by the Accreditation Auditor or auditor; iii) any misuse or abuse of privileges afforded; d) repeated violations of the accreditation policy. Depending upon the nature and circumstances leading to the de-authorization of an Identity Provider, some or all of its outstanding credentials may be revoked or transitioned to a different Identity Provider.

b) The Accreditation Authority MUST make available an appeals mechanism to allow an Identity Provider to challenge the decision to revoke the Identity Provider's status. However, for the duration of the appeal, the Identity Provider's status will remain suspended. Outcomes of an appeal MUST be reported in a transparent manner.

1.7 Accredited non-governmental entities or individuals:

a) MUST agree to:
   i. only use the data for the legitimate and lawful purpose stated;
   ii. the terms of service, in which the lawful uses of data are described;
   iii. prevent abuse of data received;
   iv. [cooperate with any audit or information requests as a component of an audit;]
   v. be subject to de-accreditation if they are found to abuse use of data or accreditation policy / requirements;
   vi. store, protect and dispose of the gTLD registration data in accordance with applicable law;
   vii. only retain the gTLD registration data for as long as necessary to achieve the purpose stated in the disclosure request.

b) Will not be restricted in the number of SSAD requests that can be submitted during a specific period of time, except where the accredited entity poses a demonstrable threat to the SSAD. It is understood that possible limitations in SSAD's response capacity and speed may apply. For further details see the response requirements preliminary recommendation.

c) MUST keep the information required for accreditation and verification up to date and inform the Accreditation Authority promptly when there are changes to this information, which MAY result in re-accreditation or re-verification of certain pieces of information provided.

1.8 Accredited governmental entities

a. Accreditation by a countries'/territories' government body or its authorized body would be available to various eligible government entities[10] that require access to non-public registration data for the exercise of their public policy task, including, but not limited to:

[10] Eligible government entities are those that governments consider require access to non-public RDDS data for the exercise of their public policy task, in compliance with applicable data protection laws. Whether an entity should be eligible is determined by a country/territory nominated Accreditation Authority, without prejudice to the final responsibility of a disclosing party for the processing of personal data following a request for RDDS data.

- Civil and criminal law enforcement authorities,
- Judicial authorities,
- Consumer rights organizations,
- Cybersecurity authorities, including national Computer Emergency Response Teams (CERTs),
- Data protection authorities

b. Eligible government entities are those that governments consider require access to non-public RDDS data for the exercise of their public policy task, in compliance with applicable data protection laws. Whether an entity should be eligible is determined by a country/territory nominated Accreditation Authority, without prejudice to the final responsibility of a disclosing party for the processing of personal data following a request for RDDS data.

Clarifying questions for the GAC Team:

2. *Does a countries'/territories' accreditation body perform all the same functions as the Accreditation Authority as outlined above, including, for example, developing an appeals mechanism, renewal, addressing abuse? If so, would the same requirements as above apply, or do specific ones need to be developed that would be applicable to governmental entities? Or would a countries'/territories' accreditation body only be responsible for confirming which national entities would be eligible for governmental accreditation, following which the Accreditation Authority would be responsible for the actual accreditation (in which the eligibility/verification part would no longer be necessary as that part of the process would be performed by the countries'/territories' accreditation body)?*

3. *As the GAC does not consist of a representative from all governments, will the GAC create a defined process that clarifies how Accreditation Authorities will be identified for each country and territory and a defined process on how government-appointed Accreditation Authorities would connect to SSAD (see also question #2).*
Note GAC comment on the Initial Report: "The GAC notes, however, that countries'/territories' chosen accreditation authorities would need to coordinate with ICANN org in order to facilitate appropriate delivery and interoperability of credentials into the SSAD. The level of safeguards are well balanced and recognize both the needs of confidentiality for certain requests, such as those made by law enforcement, and the need for appropriate levels of transparency for non-sensitive requests. The actual implementation of preliminary recommendation #2, including the arrangement with ICANN, is done by each country/territory according to their governmental and regulatory system. This includes the decision of whether the Accreditation Authority of each country/territory is limited to just one organization or applicable to multiple organizations".

4. *Some commenters have suggested replacing Consumer Rights Organizations by Governmental Consumer Protection Agencies to clearly distinguish from non-governmental organizations. Idem for the reference to cybersecurity authorities (proposed change to 'legally constituted cybersecurity authorities').*
Note GAC comment on Initial Report: "The GAC recognizes that there are non-governmental organizations/private companies commissioned by, or collaborating with governments for

pursuing public policy tasks, which should have an appropriate ability to become accredited. The issue of whether, how and when they are permitted to be accredited via a government's accreditation to the SSAD needs further consideration by the EPDP Team".

5. *Are there any scenarios in which an intergovernmental agency could be put forward for accreditation by a country/territory accreditation body?*

6. Does the first sentence of b. imply that the request and associated public policy tasks must be compliant with that country's data protection laws or any data protection law that may be applicable to data identified in a request?

7. *Depending on the response to 1, there may be a need to change the reference to 'Accreditation Authority' in the context of accreditation of governmental entities to avoid confusion with the Accreditation Authority as managed by ICANN org.*

1.9 Fees

The accreditation service will be **a not-for-profit** service that is financially sustainable. For further details, see the financial sustainability preliminary recommendation.

Implementation Guidance

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

a) Recognized, applicable, and well-established organizations could support the Accreditation Authority as an Identity Provider and/or Verify information. Proper vetting, as described in j) above, MUST take place if any such reputable and well-established organizations are to collaborate with the Accreditation Authority.

b) Examples of additional information the Accreditation Authority or Identity Provider MAY require an applicant for accreditation to provide could include:
   i. a business registration number and the name of the authority that issued this number (if the entity applying for accreditation is a legal person);
   ii. information asserting trademark ownership.[11]

Auditing / logging by Accreditation Authority and Identity Providers

c) The accreditation/verification activity (such as accreditation request, information on the basis of which the decision to accredit or verify identity was made) will be logged by the Accreditation Authority and Identity Providers.

d) Logged data SHALL only be disclosed, or otherwise made available for review, by the Accreditation Authority or Identity Provider, where disclosure is considered necessary to a) fulfill or meet an applicable legal obligation of the Accreditation Authority or Identity

[11] **For clarity, service providers and/or lawyers acting on behalf of trademark owners are also eligible for accreditation. However, such service providers and/or lawyers are acting on behalf (legally) of the trademark owner. Where such service providers and/or lawyers breach the rules of the SSAD, it is necessary that disclosing entities must be provided with such data, and it must be clear that such a breach may be considered in the future disclosures for trade mark owner on whose behalf the agent is acting. The use of different 3rd party agents cannot be used as a means to avoid past sanctions for misuse of the SSAD.**

Provider; b) carry out an audit under this policy or; c) to support the reasonable functioning of SSAD and the accreditation policy.

See also auditing and logging preliminary recommendations for further details.