GAC ACCREDITATION PRINCIPLES – 21 January 2020

The purpose of this document is to introduce to the GAC a concept paper while the EPDP Team continues to deliberate on accreditation for and access to non-public data, considering in particular expected input from European Data Protection Authorities based on ICANN's proposed Unified Access Model (see ICANN blog of 25 October 2019). This document details acceptable principles of accreditation to provide the ability to request access to registration data for governmental bodies. That enables each country/territory to provide for its bodies the ability to gain accreditation for governmental users with the required safeguards. This document will then be provided to the EPDP to ensure that governmental needs are considered before the initial report.

It should be noted that actual implementation of each item below, including the arrangement with ICANN, is done by each country/ territory according to their governmental and regulatory system.

1. **Definitions**

- Accreditation - An administrative action by which the accreditation authority declares that a party/entity user is approved to gain access to SSAD in a particular security configuration with a prescribed set of safeguards.
- Eligible 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.
- Accredited party/entity: an entity that has been accredited by an accreditation authority.
- 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 "Authorization Credentials").

- Authentication - The process or action of verifying the Identity Credential and Authorization Credentials of a Requestor.

- Credentials

    - "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 Credential 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.

- 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 Authorization Credentials 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 one or more trusted 3rd parties.
- Requestors: the entities submitting queries, the results of which gain them access to non-public gTLD registration data.
- Access Authorization – A process where an accredited entity provides its legal basis and applicable safeguards for processing personal data to meet its purpose against its identifier credential.
- Disclosing Decision - A process for approving or denying disclosure non-public registration data.

- RDDS - Registration Data Directory Services, the services that each contracted party use to collect and store domain name registration data that can be provided to access and disclosure systems such as via a System for Standardized Access/Disclosure) and WHOIS.
- Revocation of Accredited party/entity - An administrative action by which the accreditation authority revokes the credentials of an accredited party/entity who is no longer approved to operate in a particular security configuration with a prescribed set of safeguards.

- De-accreditation of Accreditation Authority – An administrative action by which ICANN org revokes the agreement with the accreditation authority following which it is no longer approved to operate as the accreditation authority.

- SSAD – System for Standardized Access/Disclosure – a system that ensures reasonable access to the non-public RDDS data for parties/entities that require legitimate access to this data.

2. Objective of accreditation

The GAC has consistently advised on the need to ensure timely access to non-public gTLD Registration Data Directory Services (RDDS) data for legitimate third party purposes that complies with the requirements of the GDPR and other data protection and privacy laws. Accordingly, a System for Standardized Access/Disclosure (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.

3. Eligibility

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

- Law enforcement authorities,
- Judicial authorities,
- Consumer right's organisations,
- Cybersecurity authorities, including national Computer Emergency Response Teams (CERTs),
- Data protection authorities,

4. Determining eligibility

Eligible 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.

5. Accreditation requirements:

In order to ensure that the accreditation procedure can provide useful information for the data controller to decide whether the RDDS data should be disclosed on the basis of a request from an accredited entity, the accreditation process should take account of a number of requirements.

The requirements shall be listed and made available to eligible entities.

Compliance of accredited entities with these requirements need to be assured by the accreditation authority. On that basis, accredited parties can be authorized to participate in the SSAD system and receive the necessary access/authentication credentials. In particular, the accreditation authority needs to ensure that an accredited entity respects the following conditions.

- Have a specific and delineated purpose for their access to and use of non-public RDDS data.
- Represent that access to and use of non-public data is for a lawful purpose and its processing will not be incompatible with the purpose for which it is sought.
- Have appropriate procedures in place to ensure appropriate identity and access management for individual users in its internal organization.
- Comply with applicable laws and terms of service to prevent abuse of data accessed.
- Be subject to, ultimately, de-accreditation if they are found to fall short or in violation of any of these requirements.
- In cases of violation of any of these requirements, be subject to penalties under applicable laws.

6. Accreditation procedure

Accreditation would be provided by an approved accreditation authority. This authority may be either a countries'/territories' governmental agency (e.g. a Ministry) or delegated to an intergovernmental agency. This authority should publish the requirements for accreditation and carry out the accreditation procedure for eligible entities.

- Accreditation emphasizes the responsibilities of the data requestor (recipient), who is responsible for complying with the law.
- Accreditation will focus on the requirements of the law, such as requirements regarding data retention length, secure storage, organizational data controls, and breach notifications.
- Renewals will incorporate updated terms of service or other obligations imposed by the accreditation authority.
- Accredited parties must provide updated accreditation materials with validity dates covering the period of accreditation.
- The accreditation authority reserves the right to update what credentials or other material are required for accreditation.

a. Renewal

Accredited/authenticated parties must renew their accreditation/authentication periodically. Each authentication authority should determine an appropriate time limit.

b. Logging

The accreditation authority must log all contact details for the accredited entities and must keep a record of any abuse by the accredited entity. This is without prejudice to any obligation the accreditation authority or the accredited entities may already have to document their use of the system.

c. Auditing

Audits should be conducted by either the data protection authority or by the country/territory designated auditor. This is without prejudice to audits that may carried out by relevant data protection authorities.

d. Complaints

Complaints regarding unauthorized access to, or improper use of, data should be handled by the accreditation authority, for which appropriate procedures should be in place. This is without prejudice to other obligations they may already have under applicable data protection laws to ensure rights of individuals are respected.

e. Data access

- Accreditation is required for a party to participate in the access system (SSAD). Unaccredited parties can make data requests outside the system, and contracted parties should have procedures in place to provide reasonable access.
- Accreditation does not guarantee disclosure of the data. The final responsibility for the decision to disclose data lies with the data controller.
- Any accredited user will be expected to only process the personal data that it needs to process in order to achieve its processing purposes. They will be obligated to minimize the number of queries they make to those that are reasonably necessary to achieve the purpose.
- Accredited entities will be required to follow the safeguards as set by the disclosing system.
- Disclosure of RDS data to the type of third parties must be made clear to the data subject. Upon a request from a data subject the exact processing activities of their data within the SSAD, should be disclosed as soon as reasonably feasible. However the nature of legal investigations or procedures may require SSAD and/or the disclosing entity keep the nature or existence of these requests confidential from the data subject. Confidential requests can be disclosed to data subjects in cooperation with the requesting authority, and in accordance with the data subject's rights under applicable law.

f. De-Accreditation

- Accredited entities will be subject to graduated penalties, and ultimately de-accreditation if they are found to abuse the system.
- De-Accreditation will occur when the accreditation authority determines that the Accredited entity has materially breached the conditions of its Accreditation based upon either; a) a third-party complaint received; b) results of an audit or investigation; or c) otherwise for any misuse or abuse of the privileges afforded.
- De-accreditation will prevent re-accreditation in the future absent special circumstances. De-accreditation procedures will be on reasonable notice to the Accredited party/entity who shall have the right to an appeal.
- De-accreditation does not prevent the requestor from submitting future requests under the access method provisioned in Recommendation 18 of the ePDP Phase 1 Report, but that they will not be accredited, and thus will be subject to delays, and manual processing.