1. Terminology

- IdP - Identity Provider
- JWT - Json Web Token
- RDAP - Registry Data Access Protocol
- TLS - Transportation Layer Security

2. Must Have Requirements

2.1 Identity Provider Accreditation and Authentication

ICANN is to accredit multiple IdPs according to need. Each user of the system is to authenticated via an IdP.

Possible Solution: Oauth2 with OpenID Connect or some aspects of them using JWTs.

2.2 Transport Security

All usages of RDAP and any other associated systems are to use TLS for HTTP (HTTPS).

2.3 Query Authorization

Each query is to be authorized by ICANN, and ICANN is to be the only entity to query Registries and/or Registrars for non-public data. Registries and Registrars are to return all available data to ICANN, and ICANN will perform the task of filtering out data according to the authorization policy.

2.4 Query Pre-Authorization

There will be a means to pre-authorize queries and obtain an access token of some nature to be used with an RDAP query.

Purpose: Pre-authorization will allow ICANN to evaluate the need of each query should policy require it, where evaluation of need is to be conducted via human analysis.

2.5 Querier Role

Each RDAP query sent by the user to the ICANN servers will contain a structured and enumerated role of the user to be used by ICANN for conducting authorization. Role information is not to be transmitted by ICANN to Registries or Registrars.

3. Nice to Have Requirements

3.1 Query Logging

ICANN's RDAP server will log each query. Every IdP will have the ability to download a query log containing only the queries of the users of said IdP. The query logs are not to be publicly available. There should be a common format for the query log.

Purpose: Query logging is one aspect of auditing the system. However, query logs cannot be made publicly available as they may jeopardize criminal investigations. Therefore, auditing on a query basis is to be conducted only between ICANN and the accredited IdPs.

Possible Solution: Using JSONLines (jsonlines.org) for an extensible and appendable format.

3.2 Query Nonrepudiation

There will be an ability to attribute each query with the user issuing the query. This attribution will distinguish each query from every other query so that each user-to-query pairing will be unique.

Purpose: This requirement will aid in the settlement of issues of abuse by users.

Possible Solution: Each query is to be cryptographically signed by the user. The signature will include both the query and a nonce. ICANN will reject any queries with signatures previously used. User agents can employ the Web Cryptographic API for signing of data. So that ICANN will not need to know the identity of the user, the IdP each query will contain the user's public key signed by the IdP. ICANN will reject any query for which the user's public key cannot be verified as validly signed by the IdP.

3.3 Public Statistics

ICANN is to publicly publish statistics regarding the queries for non-public data.