Unified Requirements

Version dated 4 February 2019

1. Overall
    a. The technologies used to implement requestor authorization MUST be based on current Internet standards.
    b. The system MUST support a distributed data model, where data is stored by the CPHs and only transferred through ICANN.
    c. All usage of RDAP and any other associated systems MUST use TLS for HTTP (HTTPS).
2. ICANN Browser-based Web portal
    a. The system MUST be able to determine whether a requestor is authorized for access to non-public data.
    b. The system MUST be able to associate attributes to the requestor, and these attributes MUST be passed by the requestor to the ICANN RDAP proxy.
    c. The system MUST provide a Web-based interface for “exceptional” requests (requests not pre-authorised) which must be submitted by, and reviewed by, a human. Once authorised, data is provided via this interface rather than via RDAP.
    d. The system MUST allow triage of requests to identify high-priority requests which must be handled first.
    e. The system MUST provide email notifications of the progress of a request through the triage-review-fulfilment process, so requestors are notified promptly of the result of their request.
    f. The system MUST assign each requestor with a unique identifier.
3. Identify Providers
    a. The technical implementation for authorization determination MAY(MUST?) be delegated to agents that are qualified and appointed by ICANN.
4. ICANN RDAP Proxy
    a. The system MUST be able to support both unauthenticated and authenticated requestors.
    b. The system MUST be able to support multiple authenticated requestor identities, each of which may be assigned a role.
    c. The system MUST be able to support multiple authorization policies based on various roles assigned to requestors.
    d. The system MUST be allow access to various data elements in RDAP based on authorization policies.
    e. The system MAY pass requestor attributes (see 2.b) to the CPH RDAP servers.
    f. The system MUST pass the requestor identifier (see 2.f) to the CPH RDAP servers.

    g. The system MUST be able to receive and redirect queries from requestors who are not authorized for access to non-public data.
5. CPH RDAP Servers
    a. The system MUST be able to receive and process queries from requestors who are not authorized for access to non-public data.
6. Logging / Auditing
    a. All data held by ICANN MUST be stored securely (including all system logs) to prevent unauthorised disclosure of requests. Consider making use of anti-phishing/MITM techniques (such as two-factor authentication, Webauthn, client certs, etc) mandatory on the web interface.
    b. ICANN's RDAP server MUST log each query. Every IdP MUST have the ability to download a query log containing only the queries of the users of said IdP. The query logs MUST NOT be publicly available. There MUST be a common format for the query log.
    c. There MUST be an ability to attribute each query with the user issuing the query. This attribution MUST distinguish each query from every other query so that each user-to-query pairing will be unique and independently verifiable.
    d. ICANN MUST publicly publish statistics regarding the queries for non-public data.
7. Performance / SLA
    a. SLA commitments for RDAP service availability and web-interface request resolution times.
    b. SLA commitments MUST be published in a transparent manner to set expectations.