Unified Requirements

Version dated 12 February 2019

1. Overall
    a. The technologies used to implement requestor identification, authentication and 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 non-public data is only transferred through ICANN.
    c. All usage of RDAP and any other associated systems MUST use TLS for HTTP (HTTPS) and other appropriate security protocols.
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 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. Authorization Determination
    a. Authorization determination MAY be delegated to agents that are qualified and appointed by the coordinating party (e.g., ICANN for gTLDs, RIRs for IP addresses).
4. ICANN RDAP Proxy
    a. The system must be able to process 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 the role assigned to the requestor, and on the query.
    d. The system MUST be able to allow granular access to various data elements in RDAP based on authorization policies.
    e. The system MUST support passing requestor *attributes* (see 2.b) to the CPH RDAP servers. Whether the system passes attributes is dictated by policy.
    f. The system MUST support passing the requestor *identifier* (see 2.f) to the CPH RDAP servers. Whether the system passes the identifier is dictated by policy.

Formatted: Heading 3 Char

Deleted: 4

Deleted:).

Deleted: email

Deleted: Identify Providers¶
The technical implementation for authorization

Deleted: (MUST?)

Commented [1]: ensure uniforming of language elsewhere

Commented [2]: Gustavo and John to ensure this is consistent throughout our documentation.

Deleted: .

Deleted: MUST

Deleted: support

Deleted: various roles

Deleted: requestors

Deleted: MAY pass

Deleted: pass

Formatted: Normal

g. The system MAY be able to receive and redirect queries from requestors who are not authorized for access to non-public data.
h. The system MUST enable automation of client requests.

5. CPH RDAP Servers
   a. The system MUST receive and respond to queries from ICANN with all available registration data.
6. Logging / Auditing
   a. Logging and audit data held by all parties MUST be stored securely to prevent unauthorised disclosure of requests.
   b. 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.
   c. ICANN's RDAP server MUST log each query. Every Identity Provider MUST have the ability to download a query log containing only the queries of the users of said Identity Provider. Whether this feature is available is dictated by policy. There MUST be a common format for the query log. The query logs SHOULD NOT be publicly available. ICANN MUST publish aggregate statistics of queries for non-public data.
   d. Data MUST be retained in accordance with requirements specified by policy.
   e. The system MUST provide the ability to reconcile queries between ICANN, CPH and requesting parties.
7. Performance / SLA
   a. There MUST be SLA commitments for RDAP service availability and web-interface request resolution times.
   b. SLA commitments MUST be published.
8. Information Security Requirements
   a. The security controls for the system SHOULD be determined and maintained based on risk assessments (for instance, Article 32 of the GDPR).
   b. ICANN and the Identity Provider MUST undergo an annual security audit by a third-party auditor and provide the audit report as requested by the interested parties.
   c. All credentials used for the system MUST adopt best current practices for credential management lifecycle (e.g. multi-factor authentication, hardware tokens, quarterly account reviews and so on).
   d. There MUST be a mechanism for reporting breaches of data privacy and security (for instance, to be in compliance with Article 3 of the GDPR).
9. Information Security Guidelines
   a. The system MUST be governed by a business continuity management program and disaster recovery/incident response plans.
   b. The system MUST be developed and operated under an appropriate systems development life cycle.
   c. Cryptographic techniques such as encryption and signing SHOULD be adopted across the infrastructure to protect the confidentiality and integrity of data at rest and data in transit.

Formatted: Heading 3 Char

Deleted: Section Break (Next Page)

Deleted: MUST

Deleted: be able to

Deleted: process

Deleted: requestors who are not authorized for access to non-public

Deleted: All

Deleted: ICANN

Deleted: (including all system logs)

Deleted: Consider making use of

Deleted: anti-phishing/MITM techniques (such as two-factor authentication, Webauthn, client certs, etc) mandatory on the web interface.¶

Moved down [1]: ICANN's RDAP server MUST log each query. Every

Deleted: 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. …

Moved down [2]: There MUST be a common format for the query log.

Deleted: ¶

Deleted: <#>ICANN MUST publicly publish statistics regarding the queries for non-public data.¶

Moved (insertion) [1]

Moved (insertion) [2]

Commented [3]: Note: We need to state that the policy group MUST specify such data retention policies, elsewhere in the Technical Model.

Commented [4]: Do we need SLA for Identity Providers and Authorization Bodies?

Commented [5]: Think through:
1. Who the SLAs apply to (ICANN Org and/or CPH)
2. Are SLAs published, and/or SLA performance published

Formatted: Normal

Formatted: Heading 3 Char

Deleted: in a transparent manner to set expectations….

Formatted: Normal