

Initial Report from the Expert Working Group on a Next Generation Registration Directory Service

STATUS OF THIS DOCUMENT

This is a report from the Expert Working Group (EWG) providing recommendations for a next generation gTLD Registration Directory Service (the “RDS”) to replace the current WHOIS system.

I. EXECUTIVE SUMMARY

The Expert Working Group on gTLD Directory Services (EWG) was formed by ICANN's CEO, Fadi Chehadé, at the request of ICANN's Board, to help resolve the nearly decade-long deadlock within the ICANN community on how to replace the current WHOIS system, which is widely regarded as "broken." The EWG's mandate is to reexamine and define the purpose of collecting and maintaining gTLD directory services, consider how to safeguard the data, and propose a next generation solution that will better serve the needs of the global Internet community. The group started with a tabula rasa, exploring and questioning fundamental assumptions about the purposes, uses, collection, maintenance and provision of registration data, as well as accuracy, access, and privacy needs, and the stakeholders involved in gTLD directory services. After working through a broad array of use cases, and the myriad of issues they raised, the EWG concluded that today's WHOIS model—giving every user the same anonymous public access to (too often inaccurate) gTLD registration data—should be abandoned. Instead, the EWG recommends a paradigm shift whereby gTLD registration data is collected, validated and disclosed for permissible purposes only, with some data elements being accessible only to authenticated requestors that are then held accountable for appropriate use.

The EWG recommends that permissible purposes include the following:

- Domain Name Control
- Domain Name Research
- Personal Data Protection
- Legal Actions
- Technical Issue Resolution
- Regulatory/Contract Enforcement
- Domain Name Purchase/Sale
- Individual Internet Use
- Abuse Mitigation
- Internet Services Provision

The EWG considered the breadth of stakeholders involved in collecting, storing, disclosing and using gTLD registration data, mapped to associated purposes. Areas of common need were then identified and taken into consideration as the EWG developed principles and features to guide the design of a next generation registration data service (RDS).

This led the EWG to consider several system designs and agree on a new registration data service model to collect, use, and disclose accurate individual data elements for various purposes. Each player in the RDS eco-system has different needs for data, different risks, and potentially different responsibilities. Historically, most of these responsibilities were transferred to the Registrars, whose primary goal was to provide working domain names to paying customers. As the Internet ecosystem becomes more complex, and with the introduction of hundreds of new gTLDs, it is likely that new players will be required to take on some of the many responsibilities that come with satisfying such a broad range of registration purposes.

The following figure illustrates the EWG's recommended model for a next generation RDS that could potentially incorporate many of the principles discussed in this report. **Key elements of this Aggregated RDS (ARDS) model include:**

- ARDS serves as an aggregated repository that contains a non-authoritative copy of all of the collected data elements
- Each gTLD registry remains the authoritative source of the data
- Requestors (users who wish to obtain gTLD registration data from the system) apply for access credentials to the ARDS
- Registrars/Registries are relieved of obligations to provide Port 43 access or other public access requirements
- In most cases, the ARDS provides access to cached registration data that is copied from gTLD registries and maintained through frequent periodic updates.
- The ARDS can also provide access to live registration data that is obtained in real-time from gTLD registries, upon request and subject to controls to deter overuse or abuse of this option.
- ARDS (or other third party interacting with ARDS) would be responsible for performing validation services
- ARDS is responsible for auditing access to minimize abuse and impose penalties and other remedies for inappropriate access
- ARDS handles data accuracy complaints
- ARDS manages licensing arrangements for access to data

ICANN contracts with an international third-party provider to develop and operate the ARDS and monitors compliance with requirements

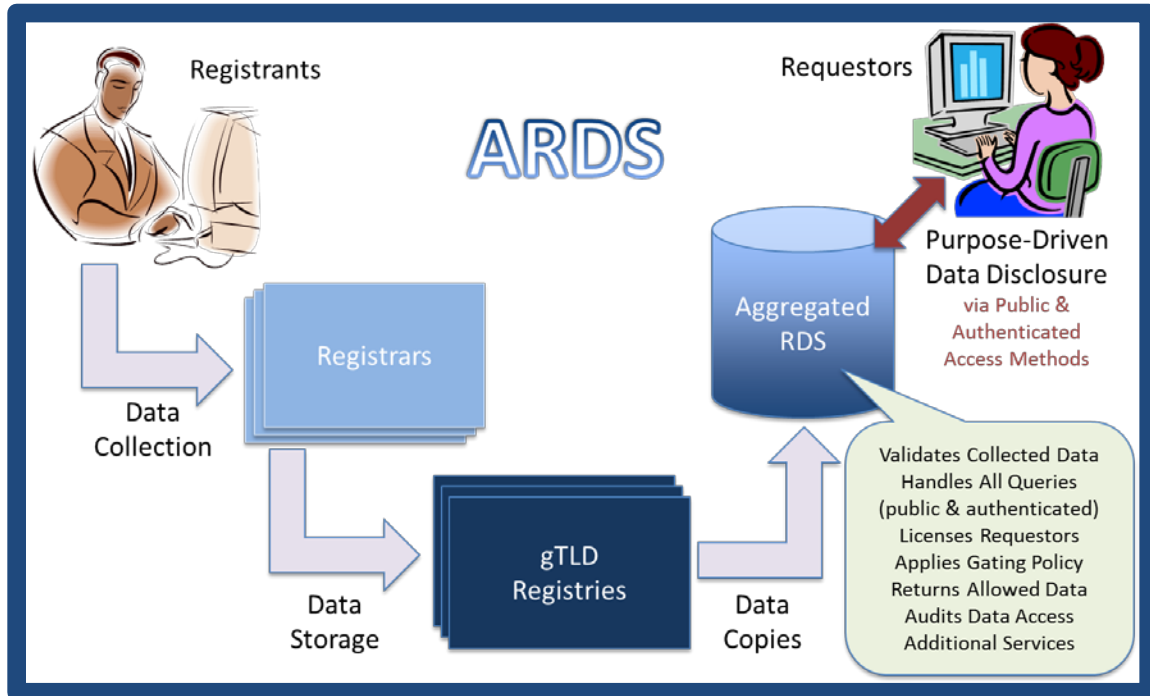


Figure 4. Aggregated RDS Model

This model received EWG members' consensus agreement because of its numerous advantages:

- Scale handled by a single point of contact
- Potential improvements in transport and delivery
- “One stop shop” for requestors of Registration Data
- Greater accountability for Registration Data validation and access (anti-abuse)
- Ability to track/audit/penalize requestors in the same way over multiple TLDs (anti-abuse)
- May reduce some costs currently borne by Registrars and Registries to provide data access
- Normalization or filtering of the data could be provided
- Reduces bandwidth requirements for Registries and Registrars
- Facilitates standardization of approaches to satisfy local data privacy concerns

- Enhanced search capability across multiple TLDs (such as reverse look-ups)
- Minimizes transition and implementation costs
- Enables validation/accreditation of requestors qualifying for special purposes (i.e., law enforcement)
- Facilitates more efficient management of inaccuracy reports
- Enables more efficient random accuracy checks
- Enables user friendly search portal displays in multiple languages, scripts and characters

Of course, nothing is perfect. The EWG also considered the following potential disadvantages to this model:

- Data Latency
- Creation of a “Big Data” source of highly valuable data with potential for misuse if not properly audited and maintained
- Increased risk of insider abuse and external attack, requiring greater attention to security policy implementation, enforcement and auditing
- Registries/Registrars no longer control delivery of registration data

In proposing this new model, the EWG recognizes the need for accuracy, along with the need to protect the privacy of those registrants who may require heightened protections of their personal information. The EWG has discussed ways in which the RDS might accommodate at-risk user needs for maximum protected registration services using “secure protected credentials.” One option might be to have ICANN accredit an independent organization to act as a Trusted Agent that, using a set of agreed criteria, would determine whether a registrant qualified for maximum protection. The EWG expects to further consider potential models for secure protected credentials which might strike an innovative, effective balance between accountability and the personal data privacy needs of at-risk Internet users.

Next Steps

Notwithstanding the progress reflected in these recommendations, the EWG has not completed its deliberations. The group seeks public input on these draft recommendations and will continue refining its recommendations as it carefully considers comments received online, at the ICANN Durban Meeting, and through other public consultation.

In addition, several key issues remain to be fully explored, such as:

- Mapping mandatory/optional data elements to each purpose
- Identifying areas requiring risk and impact analysis
- Considering costs and impacts and ways in which they might be borne
- Examining multi-modal access methods and how they could be enabled by existing or future registration data access protocols.

Following public consultation on this Initial Report, the EWG will publish and deliver a Final Report to ICANN's CEO and Board to serve as a foundation for new gTLD policy and contractual negotiations, as appropriate. As specified by the Board, an issues report based on the Final Report will form the basis of a Board-initiated, tightly focused GNSO policy development process (PDP).