

Registry System Testing 2.0



Gavin Brown
Principal Engineer, GDS Technical Services

ICANN79 TechDay
2024-03-04

What is Registry System Testing (RST)?

- Registry System Testing (RST) ensures that a Registry Operator has the capacity to operate a new generic Top-Level Domain in a stable and secure manner.
- Current service dates back to 2012; originally developed for ICANN org by IIS.
- It is now showing its age and is not able to support the Next Round:
 - manually administered (therefore fixed capacity);
 - long round-trip time to debug issues and re-run tests;
 - does not cover new registry services (i.e., RDAP).

Relevance to ccTLD registry operators

- Some ccTLDs registries are already RSPs in the gTLD space and others may consider becoming a gTLD RSP in the future.
- Any entity wishing to operate as an RSP (including for its own gTLDs) in the next round must clear RSP Evaluation, either during the RSP Pre-Evaluation phase or during gTLD application. **RST is critical for being listed as a successfully evaluated RSP, and for delegating a new gTLD.**
- Public Comment period for the RSP Handbook starts early this month (March 2024). If you are interested in participating, please consider subscribing to the [gtld-tech](#) mailing list, where ICANN org will send a courtesy message when the Public Comment opens.

Registry System Testing 2.0

- 2.0 is a new RST service that will support the next round.
 - New test plans covering all critical functions (+RDAP, -WHOIS);
 - New test plans for the RSP Evaluation Program:
 - Main RSP (EPP, RDAP, Registry Data Escrow);
 - DNSSEC RSP;
 - DNS RSP;
 - Proxy RSP.
- Passing RST is the final step before completion of RSP evaluation.
- Fully automated, self-service with an operational test and environment (OT&E).

- Once a test request has been created, the RST-API is the sole interface to provide input, manage and execute testing.
- API spec developed using OpenAPI:
 - SwaggerUI view: <https://icann.github.io/rst-api-spec/>
- This allows generation of client libraries for many programming languages.
- GitHub: <https://github.com/icann/rst-api-spec>

RST-API Endpoints

- Create a test:

POST /v1/test (*available in OT&E only*)

- Submit input parameters:

POST /v1/test/{id}/inputs (*JSON payload*)

- Upload files:

POST /v1/test/{id}/files (*multipart form data*)

- Start a test run:

POST /v1/test/{id}/run

- Review test results:

GET /v1/test/{id}

- Administration of RST can all be done on the command-line using `curl`

RST Test Plans

- Machine-readable test specification.
- Hierarchical structure:
 - A *Test Plan* uses one or more *Test Suites*;
 - A Test Suite uses one or more *Test Cases*;
 - A Test Case verifies the behaviour of a specific aspect of the behaviour of a registry service.
- YAML file is the single source of truth.
- Human-readable HTML representation:
 - <https://icann.github.io/rst-test-specs/>
- All input parameters have a JSON Schema.
- All error conditions have a unique mnemonic code.
- GitHub: <https://github.com/icann/rst-test-specs>

RSP Evaluation Tests

Main RSP	DNS RSP	DNSSEC RSP	Proxy RSP
EPP - RFC conformance - Query and transform commands - Extensions (e.g., DNSSEC, RGP) - Data persistence RDAP - RFC conformance - RDAP profile conformance IDN - IDN Guidelines conformance - IDN table review - Variant handling in the TLD and second level RDE - RFC conformance - Deposit integrity Rights Protection Mechanisms (TMCH)	Authoritative DNS - RFC conformance - IPv4/IPv6 reachability - Zone file conformance	DNSSEC Signing Maintenance of Chain of Trust DNSSEC Operations - ZSK rollover - KSK rollover - Algorithm rollover	EPP and RDAP conformance Integration with Primary SRS

Pre-Delegation Tests

1. **EPP**
 - a. RFC conformance
 - b. Query and transform commands
 - c. Extensions (e.g., DNSSEC, RGP)
 - d. Data Persistence
2. **IDN**
 - a. IDN Guidelines conformance
 - b. Variant handling in the TLD and second level
3. **RDAP**
 - a. RFC conformance
 - b. RDAP Profile conformance
4. **RDE**
 - a. RFC conformance
 - b. Deposit integrity
5. **Authoritative DNS**
 - a. RFC conformance
 - b. IPv4/IPv6 reachability
 - c. Zone file conformance
6. **DNSSEC Signing**
 - a. Maintenance of Chain of Trust
7. **Integration Test**

RST Test Plans (ctd)

- The DNS and DNSSEC test suites are based on Zonemaster.
- A Zonemaster profile is generated from the test specs and can be used to test systems locally.
- Multiple vantage points will be used to test Anycast-based DNS services. Responses must be consistent across all nodes.
- The RDAP test suite uses the RDAP Conformance Tool.
 - GitHub: <https://github.com/icann/rdap-conformance-tool>
- WHOIS, Web Whois, and Searchable Whois will not be supported in RST 2.0, as these services are being sunset in the gTLD space as of January 28, 2025.

Timeline

- Public Comment period for the API and test specs later this month (March 2024).
- Specifications will be finalised thereafter based on input received during the Public Comment period.
- Feedback can already be provided on GitHub or [gtld-tech](https://github.com/ICANN/gtld-tech).
 - RST-API: <https://github.com/icann/rst-api-spec/>
 - RST Specs: <https://github.com/icann/rst-test-specs/>
- OT&E environment will be available later this year.

Any questions or comments?



One World, One Internet

Visit us at **icann.org**



@icann



facebook.com/icannorg



youtube.com/icannnews



flickr.com/icann



linkedin/company/icann



soundcloud/icann



instagram.com/icannorg