



78

ANNUAL
GENERAL
MEETING

ICANN



1998-2023

IANA Stewardship
Transition



2016-2023



Registry System Testing (RST) Version 2.0



Gustavo Lozano
Gavin Brown

ICANN78
25 October 2023

Agenda

1. RST program
2. Estimated Timeline
3. About the RST System
4. Registry System Testing API (RST-API)
5. TLS client authentication
6. API examples
7. Testing plans

Overview - Why are we doing this?

From the [Final Report on New gTLD Subsequent Procedures PDP](#):

- **Recommendation 39.1:**
 - *ICANN must develop a set of Registry System tests designed to demonstrate the technical capabilities of the registry operator.*

- **Recommendation 39.4:**
 - *Registry System Testing (RST) must be efficient.*

Registry System Testing (RST) Program

- RST may be used to verify that:
 - a. An RSP applicant can operate in a stable and secure manner.
 - b. A gTLD has been correctly configured in the Registry Service Provider system before delegation.
- The new RST (RST v2.0) will contain only automated evaluation components.
- RST v2.0 design will be used for new and existing gTLDs when changing RSP, adding IDNs, or registry services.
- RSP and gTLD applicants will be tested on a pass/fail basis according to RST requirements.
- An Operational Test and Evaluation (OT&E) Environment will be provided.

Estimated RST Timeline

Event	Date
Implementation Review Team Review	Q1 2024
RST v2.0 Documentation Publication	Q3 2024
RST v2.0 System OT&E is ready for testing	Q4 2024
RST v2.0 System is ready for RSP applicants	Q1 or Q2 2025 (to be determined)

What Has Changed From the Existing RST System?

- New test plans to support the RSP evaluation process:
 - Main RSP (providing EPP, RDAP, RDE, optionally IDN)
 - Includes Launch Extension (RFC 8334) and TMCH coverage.
 - IDN tests will consider variants at the top- and second-level.
 - DNS RSP
 - Authoritative DNS, reachability, synchronisation.
 - DNSSEC RSP
 - Additional test suite for DNSSEC operations (ZSK, KSK, and algorithm rollovers).
 - Proxy RSP
- RDAP has been added with support for the proposed latest version of the gTLD profile to be published with the Registration Data Consensus Policy for gTLDs. RDAP tests will use the [RDAP conformance tool](#)[1].
- New test tool for EPP
 - Will allow for variable data model (e.g., minimum or full public data set) as permitted by the upcoming Registration Data Policy.
- Fully automated and API-driven.
 - No testing of port-43 WHOIS, web-based WHOIS, or searchable WHOIS.
 - Input data will be structured as JSON objects + file uploads.

RST Interaction with RSP and gTLD Evaluation

1. The testee provides a TLSA DNS RR hostname through the RSP evaluation or NSp portals for authentication and authorization of the client. For example: `tls-client-example.example.com`.
2. The testee undergoes testing in the RST v2.0 system.
3. The testee will be able see the results of the testing in the RST v2.0 system and/or the RSP Evaluation or NSp portals.
4. If testing fails, the testee can do a new round of testing in the RST v2.0 System.

RST from the Testee Perspective

1. An event occurs that triggers RST, for example: RSP Evaluation, Pre-Delegation testing.
2. ICANN org will create a new test request object in the API, associated with the TLD(s)/application in question. The test plan is fixed at this point.
3. The testee will be notified, via the respective portal, that they need to submit test input parameters via the API:
 - **POST /v1/test/{id}/files** - upload file(s)
 - **POST /v1/test/{id}/inputs** - POST a JSON object containing input parameters
 - **PATCH /v1/test/{id}** - update the test status to indicate the testee is ready for the test to begin
4. RST v2.0 system will automatically initiate a test of the applicant's system.
5. Results of the test can be retrieved from the API (**GET /v1/test/{id}**) in real-time.
6. If the test did not pass (**fail** or **error**), a re-test can be requested via the RST v2.0 system.

Registry System Testing API (RST-API)

- The RST-API will be a RESTful web service.
- The RST-API is defined using the [OpenAPI v3.1.0 specification](https://spec.openapis.org/oas/v3.1.0)[1], allowing automatic generation of client code in a wide range of languages using the Swagger tools.
- The API will also be used by ICANN org internally for integration with the RSP Evaluation and gTLD application program.
- Authentication via Mutual TLS using TLSA RRs for authenticating Network Clients (TLS-client-authentication).

TLS-Client-Authentication

- TLS-client-authentication is currently supported in [MoSAPI](#) and [RRI](#).
- TLS-client-authentication was introduced as a solution for RSPs, given the “arms length” relationship between RSPs and ICANN org.
- Large RSPs and DEAs are currently using or testing TLS-client-authentication in MoSAPI and RRI.
- More information about TLS-client-authentication may be found:
 - <https://icann.org/rri>
 - <https://icann.org/mosapi>

API Examples - Freshly Created Test

```
$ curl -s -E client.pem \  
  https://api.rst.icann.org/v1/test/987654 | jq .  
{  
  "tlds": [  
    [  
      "example"  
    ]  
  ],  
  "clientID": "tlsa.rsp.tech",  
  "testPlan": "MainRSPEvaluationTest",  
  "id": 987654,  
  "dateRequested": "2023-10-07T09:03:46.591Z",  
  "dateStarted": null,  
  "dateCompleted": null,  
  "status": "inputs-needed",  
  "result": null,  
  "inputs": {},  
  "results": [],  
}
```

API Examples - Submit Input Parameters

```
$ jo \  
  epp.hostname=epp.rsp.tech \  
  epp.port=700 \  
  | curl -s -E client.pem \  
    -H "Content-Type: application/json" \  
    -X POST \  
    -data-binary @- \  
  https://api.rst.icann.org/v1/test/987654/inputs
```

API Examples - Upload Files

```
$ curl -s -E client.pem \  
  -F file[]=@example_20231007_full_S1_R0.ryde \  
  -F file[]=@example_20231007_full_S1_R0.sig \  
  https://api.rst.icann.org/v1/test/987654/files
```

API Examples - All Input Parameters Submitted

```
$ curl -s -E client.pem https://api.rst.icann.org/v1/test/987654 | jq .
{
  "tlds": [
    {
      "example": ["latn", "ar_AR", "zh_CN", "zh_TW"],
    }
  ],
  "clientID": "tlsa.rsp.tech",
  "testPlan": "MainRSPEvaluationTest",
  "id": 987654,
  "dateRequested": "2023-10-07T09:03:46.591Z",
  "dueDate": "2023-11-07T09:03:46.591Z",
  "dateStarted": null,
  "dateCompleted": null,
  "status": "pending",
  "result": null,
  "inputs": {
    "app.hostname": "app.rsp.tech",
    "app.port": 700,
    // etc
  },
  "results": []
}
```

API Examples - Test in Progress

```
$ curl -s -E client.pem https://api.rst.icann.org/v1/test/987654 | jq .
{
  "tlds": [
    {
      "example": ["latn", "ar_AR", "zh_CN", "zh_TW"],
    }
  ],
  "clientID": "tlsa.rsp.tech",
  "testPlan": "MainRSPEvaluationTest",
  "id": 987654,
  "dateRequested": "2023-10-07T09:03:46.591Z",
  "dueDate": "2023-11-07T09:03:46.591Z",
  "dateStarted": "2023-10-07T11:16:32.041Z",
  "dateCompleted": null,
  "status": "in-progress",
  "result": null,
  "inputs": {
    "app.hostname": "app.rsp.tech",
    "app.port": 700,
    // etc
  },
  "results": []
}
```

API Examples - Test Completed

```
$ curl -s -E client.pem https://api.rst.icann.org/v1/test/987654 | jq .
{
  "tlds": [
    {
      "example": ["latn", "ar_AR", "zh_CN", "zh_TW"],
    }
  ],
  "clientID": "tlsa.rsp.tech",
  "testPlan": "MainRSPEvaluationTest",
  "id": 987654,
  "dateRequested": "2023-10-07T09:03:46.591Z",
  "dueDate": "2023-11-07T09:03:46.591Z",
  "dateStarted": "2023-10-07T11:16:32.041Z",
  "dateCompleted": "2023-10-07T18:32:12.341Z",
  "status": "completed",
  "result": "pass", // or "fail" or "error"
  "inputs": {
    "app.hostname": "app.rsp.tech",
    "app.port": 700,
    // etc
  },
  "results": [
    // detailed test results
  ]
}
```

API Examples - Test Details

```
$ curl -s -E client.pem https://api.rst.icann.org/v1/test/987654 | jq '.results[0]'
```

```
{
  "caseID": "epp-01",
  "result": "pass", // or "fail", "error" or "skip"
  "description": "successfully resolved epp.hostname for IPv4",
  "dateStarted": "2023-10-08T16:47:19.520Z",
  "dateCompleted": "2023-10-08T16:47:19.520Z",
  "log": [
    [
      "starting test epp-01",
      "resolving epp.rsp.tech/A",
      "found 1 RR(s)"
    ]
  ],
  "context": {
    "host.name": "node01.rst",
    "host.ips": "192.168.0.32, fe80::79b5:adbc:141e:b15e",
    "user.name": "rst",
    "dig.version": "DiG 9.10.6",
    "host.os": "Linux",
    "host.arch": "amd64",
    "epp.hostname": "epp.rsp.tech"
  }
}
```

Testing Plans for RSP Applicants

Main RSP	DNS RSP	DNSSEC RSP	Proxy RSP
<ul style="list-style-type: none">1. EPP<ul style="list-style-type: none">a. RFC conformanceb. Query and transform commandsc. Extensions (e.g., DNSSEC, RGP)d. Data Model2. RDAP<ul style="list-style-type: none">a. RFC conformanceb. RDAP Profile conformance3. IDN<ul style="list-style-type: none">a. IDN Implementation Guidelines conformanceb. IDN tables reviewc. Variant handling in the TLD and second level4. RDE<ul style="list-style-type: none">a. RFC conformanceb. Deposit integrity	<ul style="list-style-type: none">1. Authoritative DNS<ul style="list-style-type: none">a. RFC conformanceb. IPv4/IPv6 reachabilityc. Zone file conformance	<ul style="list-style-type: none">1. DNSSEC Signing2. Maintenance of Chain of Trust3. DNSSEC Operations<ul style="list-style-type: none">a. ZSK rolloverb. KSK rolloverc. Algorithm rollover	<p>[TBD]</p>

Testing Plans for Pre-Delegation

1. **EPP**
 - a. RFC conformance
 - b. Query and transform commands
 - c. Extensions (e.g., DNSSEC, RGP)
 - d. Data Model
2. **IDN**
 - a. IDN Implementation 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**
7. **Maintenance of Chain of Trust**

Engage with ICANN



Thank You and Questions

Visit us at icann.org

Email: email



[@icann](https://twitter.com/icann)



facebook.com/icannorg



youtube.com/icannnews



flickr.com/icann



linkedin/company/icann



soundcloud/icann



instagram.com/icannorg