Technical Update From ICANN Org

GDS Technical Services

CP Summit 2026

Agenda

1. RSP Evaluation: Second Application Window
2. MoSAPI & RRI Technical Updates
3. DNSSEC Algorithm Recommendations
4. Pre-Delegation Testing & RST v2.0
5. RST: Transition to RST v2.0
6. URS: Communication Between URS Providers & Contracted Parties

RSP Evaluation: Second Application Window

Readiness Content Disclaimer

The authoritative source for all information about RSP Program including rules, evaluations, restrictions, processes, and systems is the English version of the RSP Handbook. All New gTLD Program: 2026 Round readiness and training content is supplementary to the RSP Handbook, and has been developed to provide a high-level summary of key topic areas of interest to prospective applicants and the broader ICANN community. In case of discrepancy, the RSP Handbook prevails.

About the RSP Evaluation Program

As part of ICANN's New Generic Top-Level Domain (gTLD) Program: 2026 Round, the RSP Evaluation Program is intended to reduce the cost and time involved in evaluating new gTLDs by separating the assessment of the technical aspects of operating a gTLD from the application for the gTLD label.

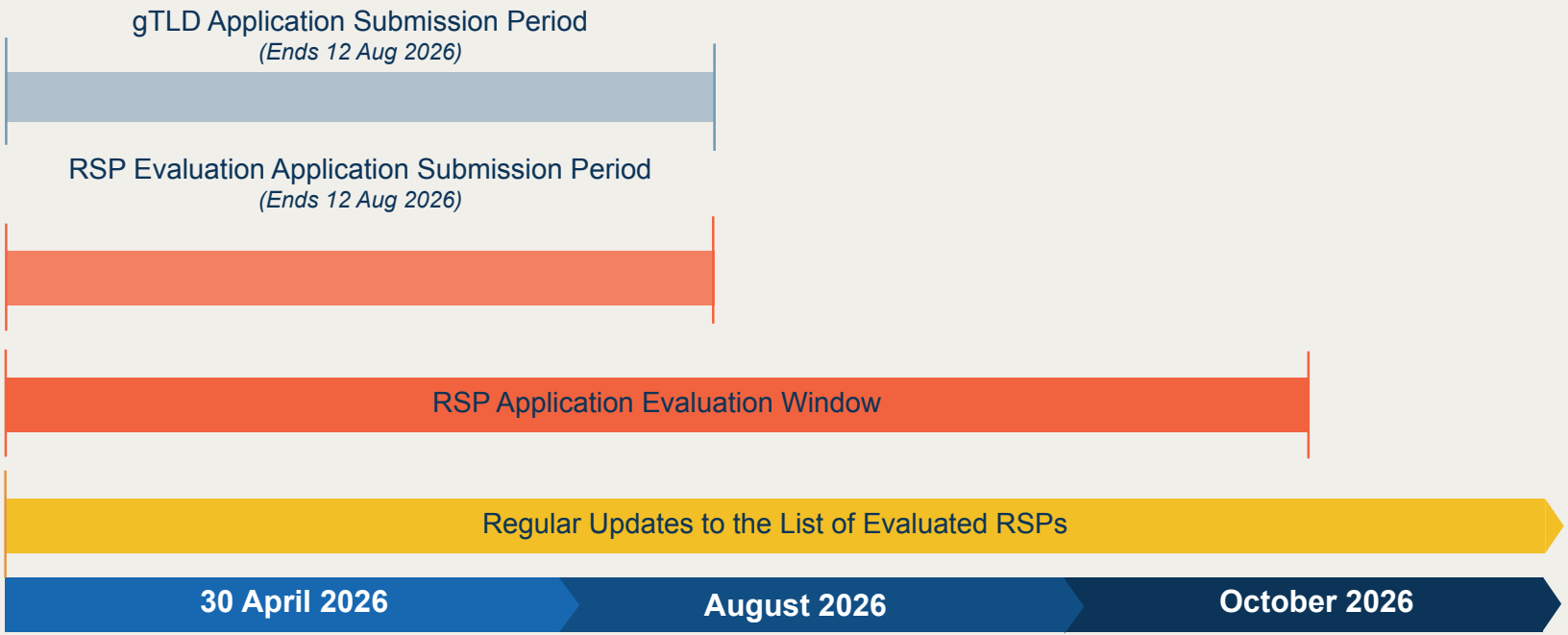
Through the RSP Evaluation Program, RSPs need only be evaluated once, regardless of the number of gTLDs they support.

All organizations must successfully clear evaluation through the RSP Evaluation Program in order to be eligible to offer services to a registry operator for any gTLD awarded during the New gTLD Program: 2026 Round.

A comprehensive list of available resources related to some of the critical technical services provided to gTLDs by RSPs can be found on the Apply to the RSP Program webpage.

RSP Evaluation Program and 2026 Round Timeline

Note: Dates are subject to change.



Who Can Apply to the RSP Evaluation Program?

Existing RSPs who did not submit an application in 2025 and new entrants.

Eligibility requirements for applicant organizations are defined in section 3.1 of the RSP Handbook.

All organizations must successfully clear evaluation through the RSP Evaluation Program in order to be eligible to offer services to a registry operator for any gTLD awarded during the New gTLD Program: 2026 Round.

What Should My Organization Do Before Applying?

1. **Read the entire RSP Handbook.** Becoming an RSP requires time and monetary commitment.
2. **Determine which type(s) of RSP application(s) is right for your organization.** An RSP applicant may apply for each type of RSP (Main, DNSSEC, DNS and Proxy).
3. **Carefully read the technical questions for the type of RSP(s) your organization will apply for** and determine if your organization can adequately provide answers to all of them.
4. **Carefully read the Registry System Testing (RST) 2.0 Specifications** as your systems will be tested as part of the RSP evaluation.
6. **Gather all necessary information about your organization** as required by ICANN to conduct legal compliance and background screening, as described in the RSP Handbook. Identify the specific users in your organization who will submit the application(s).
7. **Read the RSP FAQs.** Additional insights for applicants based on commonly asked questions and issues that other applicants have experienced.

A more comprehensive list can be found on the Apply to the RSP Program page of the 2026 Round Website.

Additional Information About the RSP Evaluation Program

RSP Evaluation Fee and Process:

- **The current RSP fee is: USD 92,000**. Per policy requirements, the fee is set to recover costs of the program.
- **An RSP may be evaluated to offer one or more types of RSP service for a single fee.**

Types of RSPs:

- **Main** (EPP, RDAP, Data Escrow)
- **DNS** (DNS Service)
- **DNSSEC** (DNSSEC Signing)
- **Proxy** (Registration Validation per Applicable Law with Proxy)

A **Main** RSP may be evaluated for one or more additional registry services (including IDN tables).

MoSAPI Technical Updates

MoSAPI Technical Updates

- MoSAPI is the system where CPs can access data collected by the SLA Monitoring system.
- Until now incident data was retained indefinitely.
- Going forward incident data will be retained for 365 days.

MoSAPI Technical Updates

- Data retention in MoSAPI

Type of data	Retention Policy (calendar days)
Incidents	365
Measurements	21
Network Troubleshooting	8

- If you need to retain it for longer you will need to download the data and retain it locally.

MoSAPI Technical Updates

- The “*nameServerAvailability*” element within a Measurement object provides the state of an “*IP address*” of a particular name server. This state can also be derived from the raw data contained within the “*testData*” element.
- The “*nameServerAvailability*” element is currently missing the “*targetIP*” element.
- Even though the raw data in the “*testData*” element within the same measurement object is complete and reflects the data in the MoSAPI back-end, the missing “*targetIP*” element makes the information in the “*nameServerAvailability*” element unusable.
- MoSAPI will be updated to include the missing “*targetIP*” element.

RRI Technical Updates

RRI Technical Updates

- Registration Reporting Interfaces (RRI) is the system used by CPs to report data escrow compliance and send reports required by the Registry Agreement.
- We are currently refactoring this interface. This will make the system faster and less prone to internal errors.
- The only visible change to CPs is that we will have some new error codes added to the spec (https://icann.org/rri).

DNSSEC Algorithm Recommendations and Operational Best Practices

Recently Published RFCs

- Per **RFCs 9904, 9905 & 9906**, DNSSEC implementations MUST NOT use the following signing and digest algorithms:
  - RSA/SHA-1 (RSASHA1, RSASHA1-NSEC3-SHA1)
  - DSA (DSA, DSA-NSEC3-SHA1)
  - ECC-GOST (GOST R 34.10-2001)
  - RSAMD5

Implications for Registry Operators

- If using RSASHA1, RSASHA1-NSEC3-SHA1, DSA, DSA-NSEC3-SHA1, ECC-GOST or RSAMD5 in your DNSSEC implementation, perform an algorithm rollover as soon as possible.
- The RECOMMENDED algorithms are:
  - RSA/SHA-256 (RSASHA256)
  - ECDSA P-256 (ECDSAP256SHA256)
  - ECDSA P-384 (ECDSAP384SHA384)
  - Ed25519 (EdDSA)

Algorithm Rollovers

- gTLD registries must at all times remain in compliance with their Registry Agreement. Going insecure is not an option.
- A Registry may safely transition to a new signing algorithm by following the procedure in Section 4.1.4 (“Algorithm Rollovers”) of **RFC 6781** (“DNSSEC Operational Practices, Version 2”).
- The `DNSSECOperationsOnly` test plan can be used in the RST v2.0 OT&E environment to test algorithm rollover procedures: if the chain of trust breaks, the test run will fail.

Pre-Delegation Testing & RST v2.0

Pre-Delegation Test Journey

- Every 2026 Round Registry Operator (RO) must pass a Pre-Delegation Test (PDT) before delegation of a gTLD in the root zone. PDT ensures that the RO is able to operate the gTLD in a stable and secure manner.
- A successfully evaluated applicant and ICANN org enter into the 2026 Base Registry Agreement.
- ICANN Org invites the new Registry Operator to provide onboarding information. This includes their RST hostname (where their TLSA record is published).
- ICANN creates the RST test object, and provides the test ID to the RO.
- The RO uses the RST-API to conduct testing, until a “pass” result is achieved. The pass result must be achieved within one year of the effective date of the RA.
- Once PDT is cleared, the RO can proceed to delegation.

Overview of RST v2.0

- RST v2.0 streamlines the RST process by implementing only automated tests and providing a fully automated, API-driven workflow.
- ROs interact with RST v2.0 through an API in a self-testing design, eliminating the need for human intervention.
- RST v2.0 was used to test applicants in the RSP Program, so all RSPs supporting 2026 Round applicants will be familiar with how it works.
- More information is available at https://icann.org/rst

How Pre-Delegation Tests Differ From RSP Evaluation Tests

		Test Suite									
		DNS	DNSSEC	DNSSEC Operations	RDAP	EPP	RDE	IDN	SRS Gateway	Minimum RPMs	Integration
Test Plan	Main RSP				✓	✓	✓	✓		✓	
	DNS RSP	✓									
	DNSSEC RSP		✓	✓							
	Proxy RSP								✓		
	Pre-Delegation Test	✓	✓		✓	✓	✓	✓*	✓*		✓

** if applied for*

How Pre-Delegation Tests Differ From RSP Evaluation Tests

- The Pre-Delegation Test covers **all** critical functions of the gTLD: DNS, DNSSEC, RDAP, EPP, and Data Escrow.
- The Pre-Delegation Test uses **production** registry infrastructure.
- The Pre-Delegation Test tests **the applied-for gTLD**, rather than an ICANN-generated TLD label.
- All IDN tables included in the application (if any) will be tested.
- All IDN variant TLDs (if any) will be tested.

How Pre-Delegation Tests Differ From RSP Evaluation Tests

- The Pre-Delegation Test includes the **Integration** test suite, which is not used during RSP evaluation. This suite confirms that the Main, DNS & DNSSEC RSPs are all interacting with each other properly in accordance with the SLA.
- The Pre-Delegation Test does not include the **DNSSEC Operations** and **Minimum RPMs** test suites, which are only used in RSP evaluation tests.
- If “Registration Validation per Applicable Law with Proxy” is included in the application, the Pre-Delegation Test will include the **SRS Gateway** test suite.
- **RSPs who cleared evaluation in the RSP Program must still pass the Pre-Delegation Test!**

Preparing for Pre-Delegation Tests

- RSPs and ROs can rehearse Pre-Delegation Tests using the RST v2.0 OT&E environment, using the `StandardPreDelegationTest` or `PreDelegationTestWithSRSGateway` test plans.
- Access to the OT&E environment is available to anyone by submission of a request to globalsupport@icann.org.
- To get access, you must publish one or more TLSA record(s) in a DNSSEC-signed zone, to authenticate with the API. Follow the instructions at https://icann.org/rst
- This page also provides links to the test plans and API spec.

RST: Transition to RST v2.0

Registry System Testing (RST)

- Registry System Testing (RST) occurs during the Material Subcontracting Arrangement (MSA) process, when an RO wishes to add or change an RSP.
- When an RO submits an MSA request, ICANN Org will coordinate with the RO/RSP to schedule a test, collect input data, etc.
- The test is then carried out manually by GDS Technical Services using the RST v1.0 test system, consisting of manual test scripts executed using command line tools.
- ICANN Org plans to transition this process to use RST v2.0.

Transition Timeline

- ICANN Org plans to notify of the migration date at least six months in advance.
- From the effective date, all MSA-related RST tests will use RST v2.0 and RST v1.0 will be retired.
- RST v2.0 will use the “RSP Change Test” test plan (`StandardRSPChangeTest`)

RST v2.0 & Existing RSPs

- Existing RSPs who were not evaluated in the RSP Program may not be familiar with RST v2.0.
- Access to the OT&E environment is available as described in previous slides.
- RST v2.0 was designed to test 2026 Round RSPs and gTLDs, and the rules these must follow are the default configuration for RST v2.0.
- In production tests, ICANN Org will ensure the correct configuration to avoid false positive fail results when testing existing gTLDs & RSPs.

URS: Communication Between URS Providers & Contracted Parties

Current URS Requirements

- ICANN Org is reviewing the URS Technical Requirements, following the **PDP Review of All Rights Protection Mechanisms in All gTLDs**.
- Authentication of messages sent to registries and registrars by URS providers is essential to **avoid malicious requests to lock, unlock, suspend or restore domain names**.
- As of now, communications from URS Providers must be digitally signed using **OpenPGP** (RFC 4180). ICANN provides the **URS Provider PGP Keys (URSPK)** to registries and registrars, who must use the URSPK to verify the signatures on email from URS providers.
- ICANN Org has identified two changes to the Technical Requirements, relating to:
  1. encryption of Registration Data sent by contracted parties to URS Providers;
  2. the use of OpenPGP to provide authenticity of messages sent to contracted parties by URS Providers.

1. New Requirement to Encrypt Registration Data

- Registries (and registrars, where the gTLD operates a minimal data set) MUST provide Registration Data (including non-public elements) to URS providers upon instruction.
- To comply with data protection best practices, this data MUST be encrypted, so that only the URS provider can access it.

2. Issues with OpenPGP

- Through the years, a few technical issues have been identified with OpenPGP regarding its use in URS proceedings:
  - **Interoperability:** GnuPG (a common implementation) will not implement the new version of OpenPGP (RFC 9580), meaning that users of other OpenPGP implementations may not be able to securely communicate with GnuPG users, and vice versa.
  - **Usability:** very few mail clients natively support OpenPGP, making it hard for non-technical users to install and use.
- OpenPGP's issues have prompted ICANN Org to propose changing the system used to the **integrity** and **confidentiality** of URS proceedings.
- The solutions investigated were S/MIME and an ICANN-operated proprietary solution.

Solutions Comparison

Feature	OpenPGP	S/MIME	Proprietary solution
End-to-end security	Yes	Yes	No
Confidentiality	Yes	Yes	Yes
Integrity	Yes	Yes	Yes
Built-in support in popular mail clients	No	Yes	No
Easy to use (by non-technical users)	No	Yes	No
Amount of engineering required to support*	Medium	Low	High
TCO to operate*	High	Medium	High

** on the part of URS Providers and Contracted Parties*

Proprietary Solution

- URS participants would transmit messages using symmetrically encrypted files (eg .pdf or .zip files) attached to emails.
- ICANN Org would provide a clearinghouse for the decryption passphrases, via the RRI (https://icann.org/rri).
- ICANN Org would never see the ciphertext of messages sent between participants in the system.
- To decrypt a message (and prove its authenticity), the recipient would query the RRI for the passphrase associated with the (unique) encrypted file name, and decrypt the file.
- Ultimately, this approach was not assessed as preferable to an end-to-end model.

S/MIME Support

- S/MIME is fully supported (encryption, decryption & verification, no plugin required) in the following MUAs:
  - Outlook (Windows & Mac)
  - Apple Mail.app (macOS & iOS)
  - Thunderbird (many platforms)
  - Google Workspace (workspace admin to must enable it)
- S/MIME signature verification (no encryption/decryption) is supported in Gmail.

Access to URS Contact Lists

- ICANN Org publishes a URS Contact List on https://urs.icann.org.
- For S/MIME, this list is needed by CPs to identify *which* email addresses are authorized to send lock/unlock/suspension messages, and requests for Registration Data.
- Access to the list is protected by HTTP authentication (username and password).
- Registry Operators provide access credentials during NSp onboarding.
- In the future, the RRI could replace https://urs.icann.org as the way to access the URS Contact List.

Next Steps

- Continue the conversation. Question for the audience: in what forum?
- No firm transition timeline has been determined, but contracted parties will be given advance notice with sufficient time to make any changes needed to support the new requirements.

Thanks!


icann.org


@icann


facebook.com/icannorg


youtube.com/icannnews


flickr.com/icann


linkedin.com/company/icann


instagram.com/icannorg