

# Updates to the Root Zone Management System (RZMS)

**Kim Davies, VP, IANA Services**

**Amy Creamer, Director of  
Operations, IANA**

**George Sarkisyan, IANA Services  
Sr. Specialist**



# Why we are here today

---

- ❑ The Root Zone Management System (RZMS) has been in operation for over a decade and has served us well
- ❑ ICANN has invested in improving the system in recent years to better cater for evolving and future needs
- ❑ The first significant upgrade resulting from these efforts is planned for later this year, and will introduce some changes to customers that we wish to share and discuss.
- ❑ The IANA team is on-site throughout the week to meet with customers and work with you on your unique situation

# Brief History on Root Zone Management

---

- ❑ Root Zone Management has been a responsibility of ICANN, through the IANA functions, since ICANN was first created in the late 1990s
  - ❑ Prior to this, it was operated as part of the InterNIC services which also included .com/.net/.org registrations and some IP address allocation services.
  - ❑ Jon Postel/IANA was consulted on root zone changes and other policy adjudication questions by InterNIC staff.

# Brief History on Root Zone Management

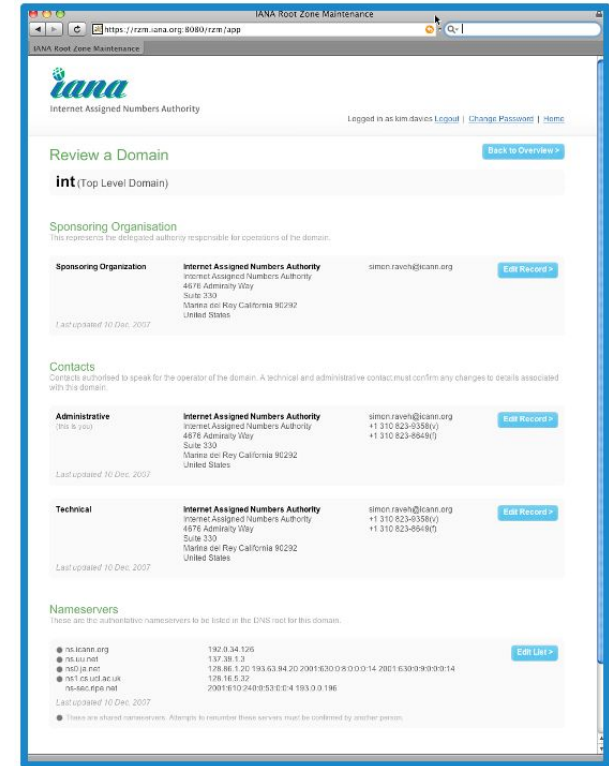
- Historically root zone changes were manually processed from beginning to end.
- Internal processing often involved printed checklists and paper documents exchanged with customers.
- In the early 2000s, both ICANN and community recognized the benefits of increased automation and initiated activities to realize it in day-to-day operations

A photograph of a handwritten checklist for root zone management. The checklist is titled 'TLD or Country Code' and lists various steps and their completion dates. The document is dated 9/20/04 and includes a tracking number #20040902173. The checklist is marked with checkmarks and handwritten notes.

Task	Date/Status
TLD or Country Code	CA
Name or Country Name	CANADA
Tracking Number	#20040902173
Request sent to IANA	9/2/04
Request confirmed received	9/2/04
Print ICANN-REG IANA Whois	9/2/04
Are there any special procedures?	✓
Check Root-Zone Information	N/A
Does this request affect other TLDs?	✓
Clarification communications begin	N/A
Clarification communications end	N/A
Requested Changes	N/A
Message to AC & TC	US
AC - Verification	9/2/04
TC - Verification	9/2/04
PAC - Verification (if needed)	9/5/04
PTC - Verification (if needed)	N/A
IANA Procedures have been met?	N/A
Technical check complete (IPv4)	6/2/04 9/6/04
Technical check complete (IPv6)	6/2/04 9/9/04
Message to DoC and Verisign	N/A
Approval from DoC	9/6/04
Notification from Verisign	9/6/04
IANA Website changes (Yes/No)	9/1/04
Check for shared contacts	NO
IANA Website changes complete	N/A
Check Root Zone for completed changes	N/A
Confirm with ACTC changes completed	2x #20040902
Entries in Database complete	9/15/04
Notes: * Robin set Release from US63 until 9/15/04 after signature - not sure why it didn't come through.	
Request Completed	
Is there another request to start pending this request's completion?	FILE
	No

# Brief History on Root Zone Management

- ❑ In 2006, ICANN kicked off implementation of the Root Zone Management System (RZMS)
  - ❑ Workflow management system that would handle root zone changes end-to-end
  - ❑ Integrated with a like-minded system built by Verisign for their component
  - ❑ ICANN's system iterated upon a proof-of-concept developed by the .PL registry NASK as part of a CENTR initiative.
- ❑ RZMS was first launched on 22 July 2011



- ❑ All TLD managers can use it to perform common maintenance tasks for their TLDs
  - ❑ Self-service portal
  - ❑ Streamlined processing
- ❑ Successfully evolved to support new requirements
  - ❑ Signed delegations/root zone
  - ❑ Removing NTIA's role after IANA transition
  - ❑ Integration with ICANN org NSP portal for TLD delegations
- ❑ Particularly complex tasks still done out of band (e.g. ccTLD transfers), ticketing system still used for correspondence

# The need to evolve

---

- ❑ We have customers with new usage patterns that weren't envisaged in mid-2000s, e.g. large portfolios, frequent key rollovers
- ❑ Technical architectural choices in the original prototype limit the flexibility of the current system to continue to evolve
  - ❑ ICANN recommended a complete rebuild to a modular architecture
  - ❑ Modular architecture will also more targeted evolution of components rather than monolithic upgrades in the future
  - ❑ We also reached a limit to how much we can optimize certain workflows like technical checks due to lack of parallelism
- ❑ We had ideas to increase customer utility (evolved authorization model, security improvements, technical check evolution, adding APIs, etc.)

## What's new in the upgraded RZMS?



# TLD Authorization Model – Changes

## Current

### Administrative Contact

- 1 Listed in public WHOIS
- 2 Approves change requests
- 3 Must be in country (ccTLDs)

### Technical Contact

- 1 Listed in public WHOIS
- 2 Approves change requests

## New model

### Administrative Contact

- 1 Listed in public WHOIS
- 2 Public information only, not used for authorisation
- 3 Must be in country (ccTLDs)

### Technical Contact

- 1 Listed in public WHOIS
- 2 Public information only, not used for authorisation

### Credentialed Users

- 1 Not published (managed via RZMS)
  - 2 Submits and/or approves change requests
- 
- One or more (no fixed number)
  - Must be persons (no role accounts)
  - Stronger identity controls
  - Flexible threshold approval options

*Transition process*

# TLD Authorization Model – Increased Flexibility

---

- ❑ TLD managers can now add additional people to interact with IANA, and set custom levels of responsibilities for each.
- ❑ This provides managers the flexibility to create as many individual user accounts and configurations as needed for change request approvals.

# Every User Gets Their Own Account

---

- ❑ Each individual user will be issued their own account
  - ❑ Important to complete your profile information for credential recovery situations
  - ❑ A Contact Name is required, though you may use a role account email (not recommended)
- ❑ User approvals performed after secure login
  - ❑ Tokens transmitted via email no longer used for authorization purposes
  - ❑ Improves security at the cost of reduced flexibility

# Customizable User Roles

Each user can be configured with different combinations of roles and responsibilities

## Change of Control

Such as changes to the registry operator

## Non-Technical

Such as changing public contact information

## Technical

Such as adding/removing NS or DS records

## Authorization Policy

Such as adding/removing users and changing approval thresholds

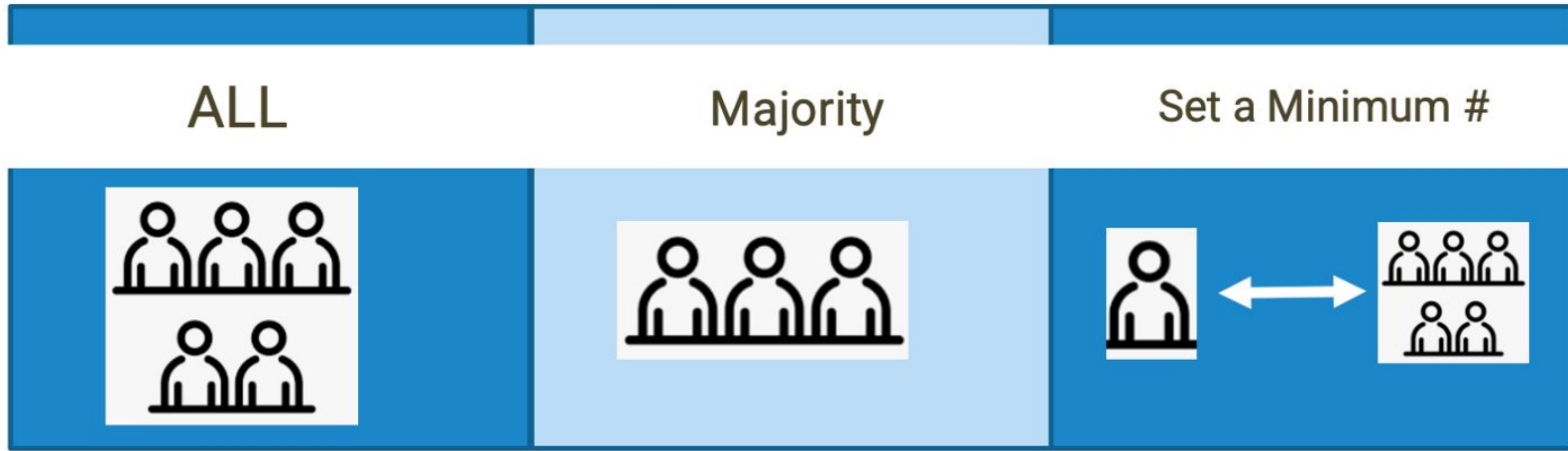
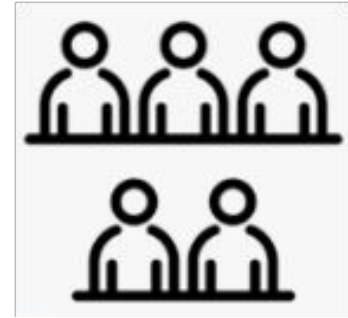
# Approval thresholds

---

- ❑ Thresholds allow you to customize the number of users who need to approve each type of change
  - ❑ Currently both the Administrative and Technical Contacts must cross-authorize changes, now you have flexibility.
  
- ❑ Approval threshold options:
  - ❑ All (i.e. all users who can approve that type of change)
  - ❑ Majority
  - ❑ A specific number (user-defined)

# TLD Authorization Model – Threshold Example

Five users have permission to approve technical changes. When a technical change request is submitted, the threshold setting determines how many of those users must approve that request:



# Submit More Than One Request

---

- ❑ Previously, only one change request could be active per TLD at the same time.
  
- ❑ Now, multiple change requests can be active per TLD
  - ❑ Requests must not impact the same data section
  
- ❑ Multiple changes can *still* be made on one request
  - ❑ If different request types are in the same request (example, technical or non-technical) the request must be approved by user(s) with the appropriate authority

# Activity Log

- ❑ Tracks a request through the different phases
- ❑ Shows previous reports of tech checks, which re-run every six hours
- ❑ Shows which user approved the request with a timestamp
- ❑ Shows which user submitted the request

❑	2022-09-06 23:00:07	<a href="mailto:root-mgmt@iana.org">root-mgmt@iana.org</a>	has opted in (acknowledged) to being a public contact for .tld1
❑	2022-09-06 22:58:29	<a href="#">Amy Creamer</a>	has approved request
❑	2022-09-06 22:57:47	<a href="#">System</a>	sent notification to new public contact for .tld1
		Amy Creamer <root-mgmt@iana.org> Technical Contact <tld-contact@iana.org>	
↔	2022-09-06 22:57:46	<a href="#">System</a>	Request entered Contact Confirmation
❑	2022-09-06 22:52:59	<a href="#">System</a>	has completed technical check - <b>bfb3673f-7665-4ff7-aabe-0c33078767a3</b>



- ❑ The system will provide a new overview of technical checks, with the ability to drill down into specifics

Technical check results from 2022-08-31 00:55:06 <a href="#">Click here to view Full Technical Check Log</a>		<b>Fail</b>
<b>Test Results</b>		
<b>Minimum number of name servers</b> Checks a domain must have at least two name servers and they are not resolved to the same IP address. <a href="#">Click for more details &gt;</a>		<b>Pass</b>
<b>Valid hostnames</b> Checks that hostname comply with the requirements described in RFC 1123. <a href="#">Click for more details &gt;</a>		<b>Pass</b>
<b>Name server reachability</b> Checks that each name server is reachable by UDP and TCP. <a href="#">Click for more details &gt;</a>		<b>Fail</b>
<b>Answer authoritatively</b> Checks that each name server is authoritative for the designated zone. <a href="#">Click for more details &gt;</a>		<b>Fail</b>

The technical check process has been separated into its own independent infrastructure for these benefits:

- ❑ Technical checks can be scaled to increase throughput and optimize performance
- ❑ Technical checks can easily be evolved

# Application Programming Interface (API)

---

- ❑ TLD managers can build or use tools to programmatically communicate with RZMS
- ❑ Initial features focus on bulk updates by registry operators, who manage multiple TLDs and need to perform change operations efficiently

- ❑ Submitting a change request
- ❑ Adding new users
  - ❑ Selecting their approval categories
  - ❑ Setting thresholds
- ❑ Sending an invitation
- ❑ Retesting technical issues
- ❑ Approving a change request

# What we're working on next in RZMS

## TLD Manager API

Enhancements to the TLD Manager API including use of secure API tokens for authentication

## Multi-Factor Authentication (MFA)

Secure logins with TOTP - e.g. Google Authenticator - as a second factor authentication for TLD Managers

## Technical Check Warnings

Technical check warnings for some checks are acknowledged by TLD Managers for the request to proceed to implementation

---

# Q&A

- ❑ IANA Community Day, 17 November 2022 at ICANN DNS Symposium 2022
  - ❑ <https://www.icann.org/ids>
  - ❑ Evolution of technical checks
- ❑ Email us RZMS related questions at [iana@iana.org](mailto:iana@iana.org)



# Thank You and Questions

Visit us at [icann.org](https://icann.org)



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



[facebook.com/icannorg](https://facebook.com/icannorg)



[youtube.com/icannnews](https://youtube.com/icannnews)



[flickr.com/icann](https://flickr.com/icann)



[linkedin/company/icann](https://linkedin/company/icann)



[slideshare/icannpresentations](https://slideshare/icannpresentations)



[soundcloud/icann](https://soundcloud/icann)