Evolving the Root Zone Management System

Kim Davies
VP, IANA Services; President, PTI

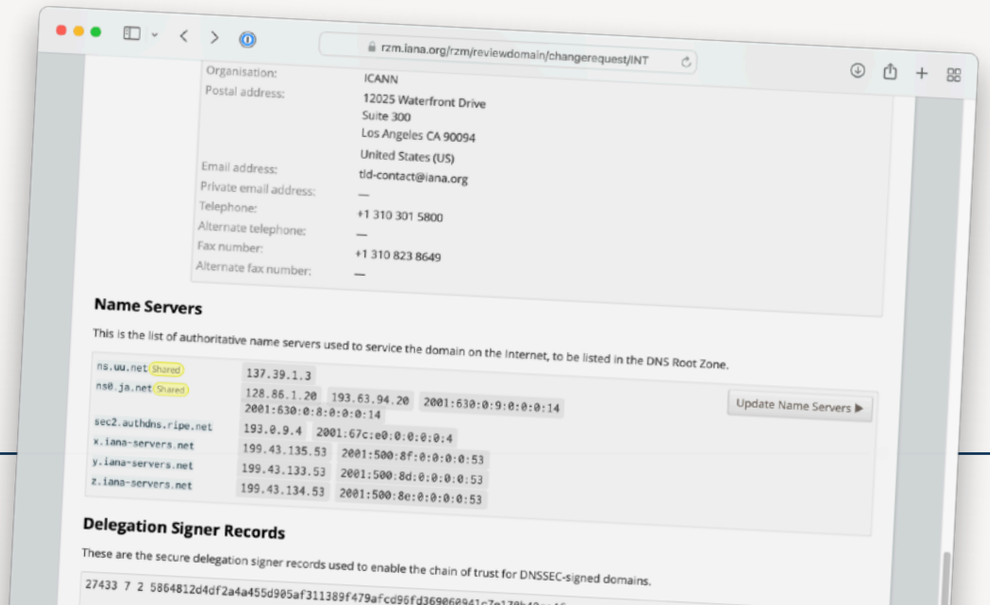
PTI | An ICANN Affiliate

Introduction

- Later this year we plan to introduce our next-generation Root Zone Management System
  - Will introduce some important evolution of some aspects of root zone management
- Our roadmap will see additional features coming beyond the first release
- We are also looking at evolving other technical aspects of root zone management

What is RZMS?

- Manages the workflow of most root zone change requests from submission through to implementation
- Provides a self-service portal for TLD managers to log in, submit requests, provide responses and check status
- Integrates with other related systems
  - the Root Zone Maintainer (Verisign) via EPP to send root zone deltas for publication
  - the NSP portal provided by ICANN org to gTLDs for new TLD workflows
- Traces its lineage back to an experimental proof-of-concept developed by CENTR/NASK 20 years ago

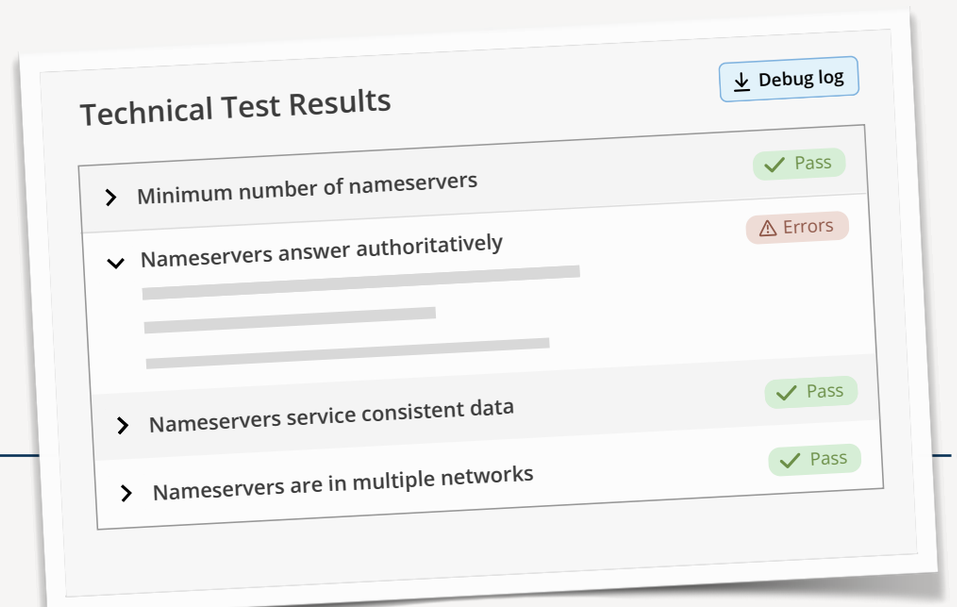


The need for change

- The platform has incrementally grown, but is constrained in supporting future needs
- When it was created
  - Most TLD managers operated only 1 domain
  - No smartphones (WAP was state-of-the-art)
  - NTIA relationship
  - Architecture and frameworks from the early 2000s, no longer modern
- Identified pain points for staff and customers
  - Original InterNIC contact model strained
    - Increasing use of ‘role’ accounts and manual interactions with IANA staff to address complex operational requirements
    - Public POCs are a marketing/spam magnet
  - Not well suited to bulk updates
- Post-transition IANA has more flexibility to support needs

What's new this year?

- **Complete platform rewrite**
  - Ground up with modern architecture, in-house by ICANN E&IT department
- **Technical check system**
  - A new standalone microservice that implements technical checks independently of RZMS via an API
  - Scalable/parallelizable
  - Can be updated on its own cadence without monolithic updates to RZMS
  - Provides comprehensive (debug-style) logging to enable customer to dive deep into any failures
  - Richer explanations that should be more intuitive



What's new this year? (2)

- **Authorization model**
  - Move to a flexible model where TLDs can appoint any number of users to manager their TLD with IANA
  - Each user can be set with different privilege levels
    - Should enable TLD manager delegating limited access to their RSP vendor for common operations
  - Users will be tied to individuals not roles, allow better security practices
    - Admin/Tech contact retained as public information only (i.e. WHOIS/RDAP)
- **Streamlined approvals for shared glue**
  - Currently, require all affected TLDs' contacts to positively consent to a change to shared glue
  - New model: submitting TLD consents, other impacted TLDs are notified and given a 14 day window to object, otherwise request proceeds.

Introduction to RZMS session
Tuesday 10:30 MYT, Room 304-305

What’s coming beyond?

- **API access**
  - Programmatic capability to submit and interact with change requests
  - Aims to cater for the needs of bulk users in particular (e.g. RSP-level key rollovers and contact changes)
  - HTTP endpoint, JSON payload, access with revokable tokens issued via web UI
- **Pass/fail/warn**
  - Ability to classify certain technical check issues as “warnings”. Will block progress of request but can be self-dismissed by customer without IANA staff involvement.

What's coming beyond? (2)

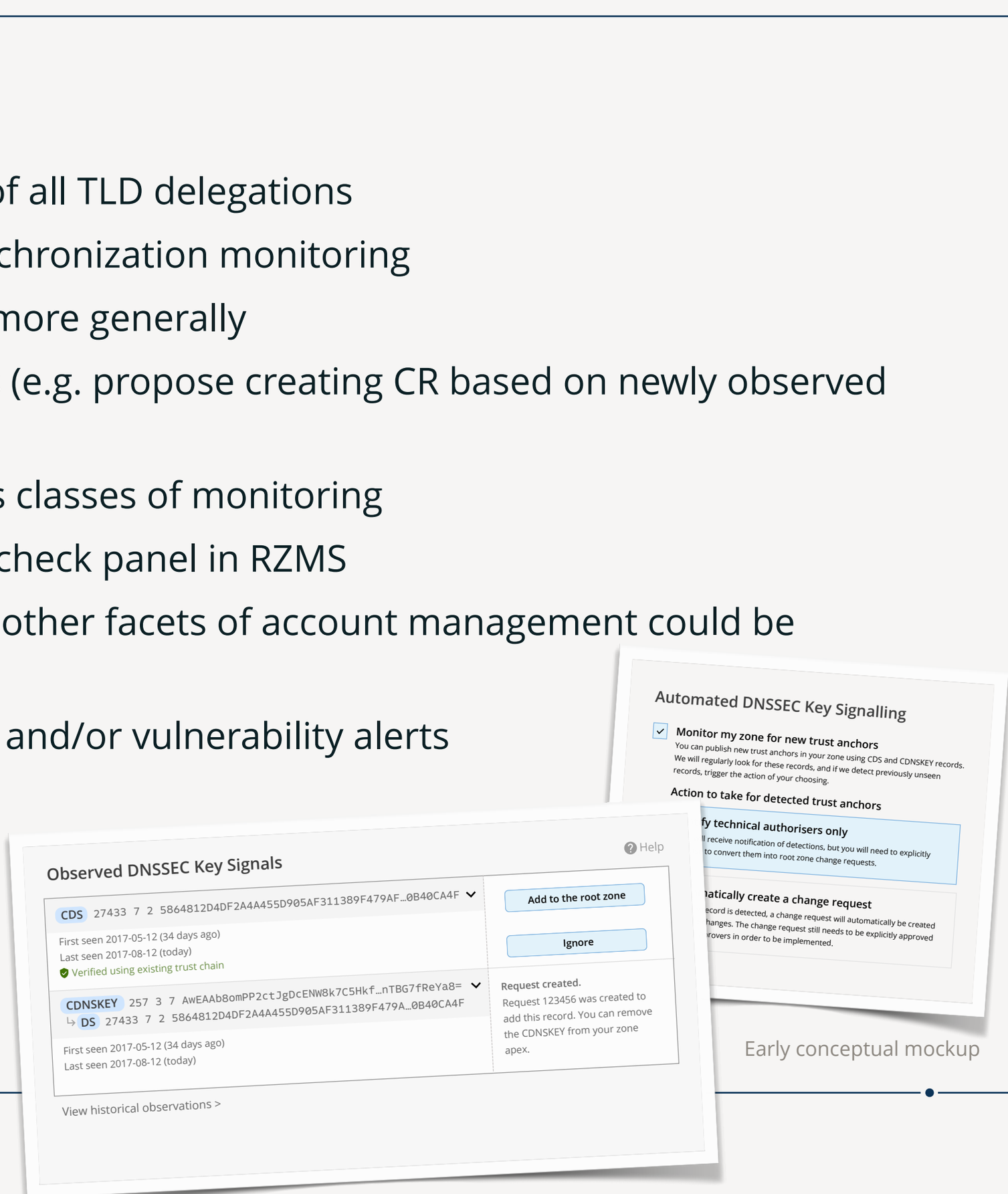
- **Multifactor authentication**
  - Have conflicting advice on this (e.g. SSR2 versus Root Zone Update Study)
  - At its heart, concern is very low interaction model and likelihood of customer staff turnover and/or credential loss
    - Becomes an operational challenge to do "trust reboots", requires robust KYC procedures we do not have today
    - Also need a model that works for customers from *every* country
  - Limit third party dependencies
    - Favours TOTP and WebAuthn, limits SSO options, no cell phones
  - How does our "proof of possession" approach factor into this?
    - A current powerful "what you have" factor is the ability to exhibit your root zone change in the apex of your zone (i.e. NS records, DNSKEY records).
    - If you have access to the zone already, you already have fundamental access to the registry without IANA enabling it

Evolving our operations

- **Technical Check Evolution**
  - We believe it is now a good to re-evaluate how we perform conformance testing (“tech check”) for root zone changes.
    - Current set largely stems from 2007 public comment period
  - Root Zone Update Study provided some important inputs
  - We’ve received general feedback over the years on suggestions from customers for refinement.
  - With pass/fail/warn system in place we can check for other discretionary things that aren’t necessarily request “blockers”, but best practices or signs of potential misconfiguration

Evolving our operations (2)

- **Proactive testing**
  - Proactive regular monitoring of all TLD delegations
  - Expanding upon just child synchronization monitoring
    - Notify of emerging issues more generally
    - Provide actionable triggers (e.g. propose creating CR based on newly observed NS-set or CSYNC records)
    - Ability to mute or suppress classes of monitoring
  - Summarize issues in a health-check panel in RZMS
    - Beyond delegation health, other facets of account management could be aggregated
    - Password/credential aging and/or vulnerability alerts
    - Validate contact methods



Early conceptual mockup

Engagement kickoff

- Adjacent to the **ICANN DNS Symposium**, we will be holding a session on IANA technical evolution
  - https://www.icann.org/ids
- Two key themes will be:
  - Tech Check Evolution
  - Algorithm rollover for the DNS root zone
- Encourage your participation there, as we flesh out our thoughts in more detail
- Will also do online engagement, public comment periods and the like, throughout the process so there will be ample opportunity to contribute.
- But thoughts are welcome any time (including now!)

IANA Community Day
17 November 2022, Brussels

Thank you!

kim.davies@iana.org