Technical Roadmap for Root Zone Management

ICANN DNS Symposium: Madrid, Spain
13 May 2017

PTI | An ICANN Affiliate

Root Zone Management

- We manage the root zone and associated database, which is comprised of the official record of top-level domains and the technical delegation data.

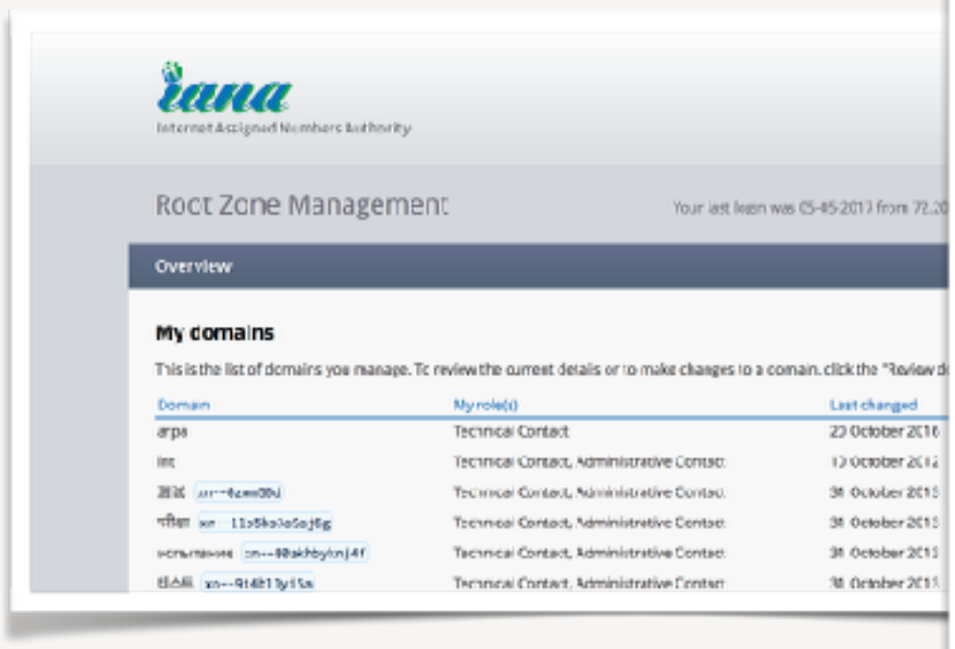
- We provides interfaces to TLD operators to perform changes, such as routine updates as well as transfers.

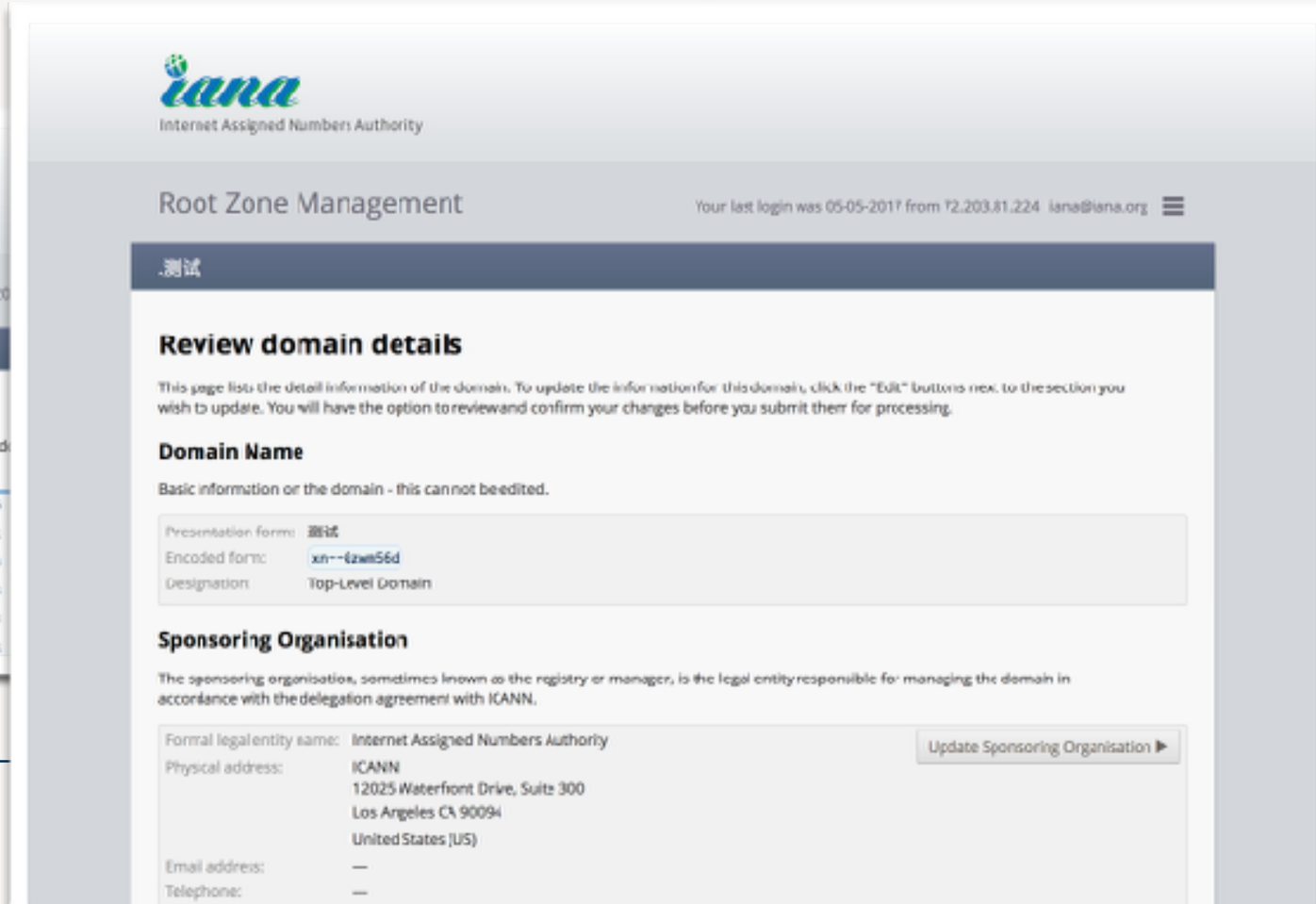
- We review all changes, ensure they meet technical and operational requirements, and are consented by the right parties. We send validated root zone file changes to Verisign as the Root Zone Maintainer to publish delegation data changes to the root servers.

- Much of the mechanisms and practices associated with the root zone are inherited from many decades of operation.

Root Zone Management System

- Around ten years ago, the Root Zone Management System (RZMS) was released.
- Provides self-service capability for TLD managers, and manages the entire workflow of change requests through stages of processing.
- Prior to RZMS, root zone workflow was fully manual.
- Major changes to date: DNSSEC, New gTLD Program and IANA stewardship transition





Root Zone Management System Roadmap

Planned updates to existing system

New automated workflows

New DNSSEC algorithm support

Next-generation rearchitecture

New authorization model

New technical check implementation

New customer API

New security options

FOI implementation

New automated workflows

- Routine change requests are currently sent between PTI and Verisign via EPP.
- Three business processes are still manually communicated:
  - Changes to the authorities for the root zone
  - Deletion of a TLD
  - Escalation of a change request to be an “emergency”
- Aim is to have 100% of interactions communicated via EPP later this year
  - Stipulated in the Root Zone Maintainer Agreement

New DNSSEC algorithm support

- Current suite of algorithms were those supported in 2010 with comprehensive software support.
- New algorithms, particularly associated with elliptic-curve cryptography, are now available.
- Aim is to support new algorithms and digests as mature implementations are available.
- Deprecating algorithm and digest types to be left for future consultation on technical checks.
- Under active evaluation by development teams.
- Should we consider whether to allow untestable algorithm types in the root zone?

Algorithm Types
DSA/SHA-1
RSA/SHA-1
DSA-NSEC3-SHA1
RSASHA1-NSEC3-SHA1
RSA/SHA-256
RSA/SHA-512
GOST R 34.10-2001
ECDSA P-256 SHA-256
ECDSA P-384 SHA-384
EdDSA 25519
EdDSA 448

Digest Types
SHA-1
SHA-256
GOST R 34.11-94
SHA-384

New authorization model

- New mechanism to address pain points our customers see with the current method of submitting and approving root zone change requests.
- Find a mechanism that is flexible to allow for different configurations.
- Key foundation is decoupling the “authorization” and “published contacts” pieces of being a TLD contact.
- Seeking feedback as we commence development.

New authorization model

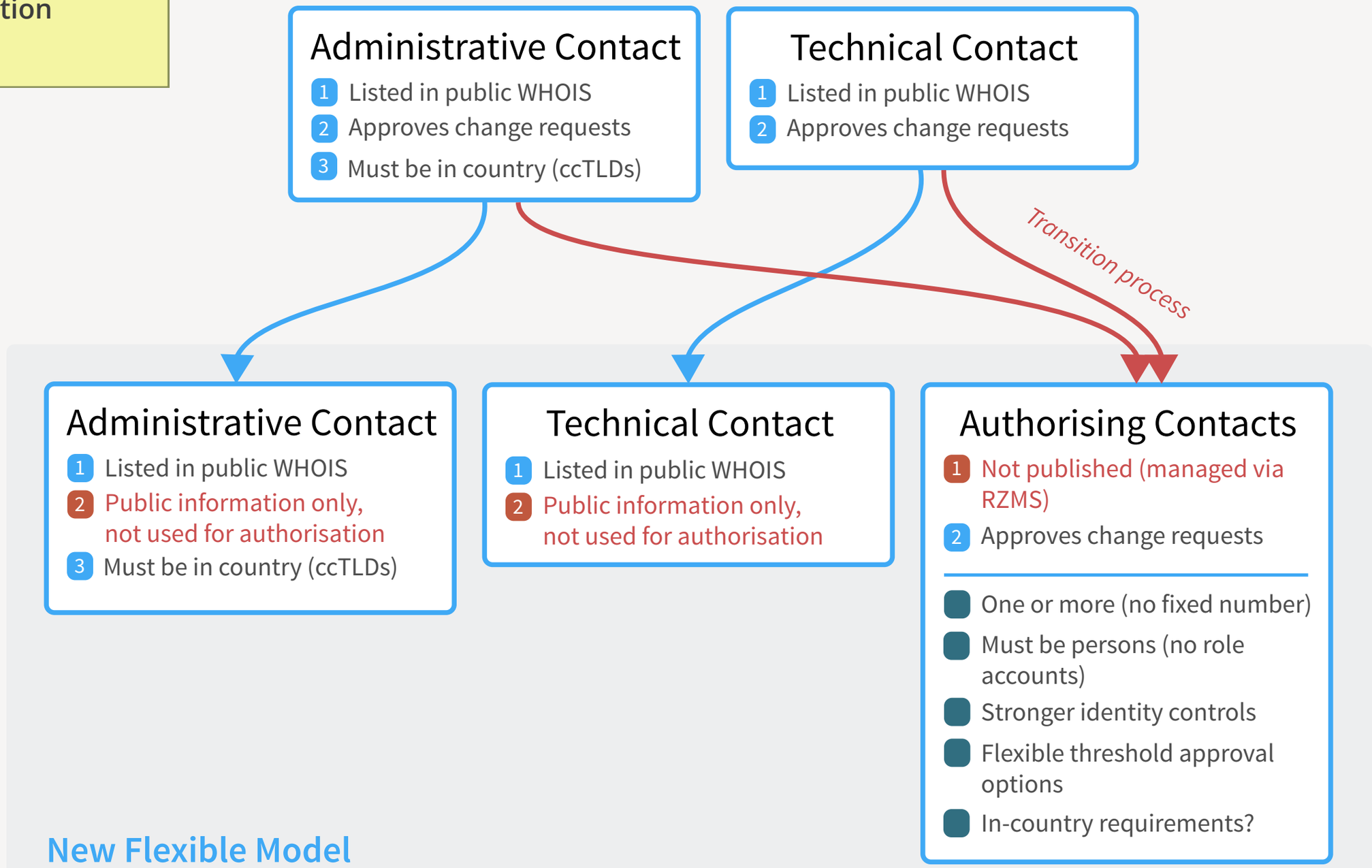
Administrative Contact

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

Technical Contact

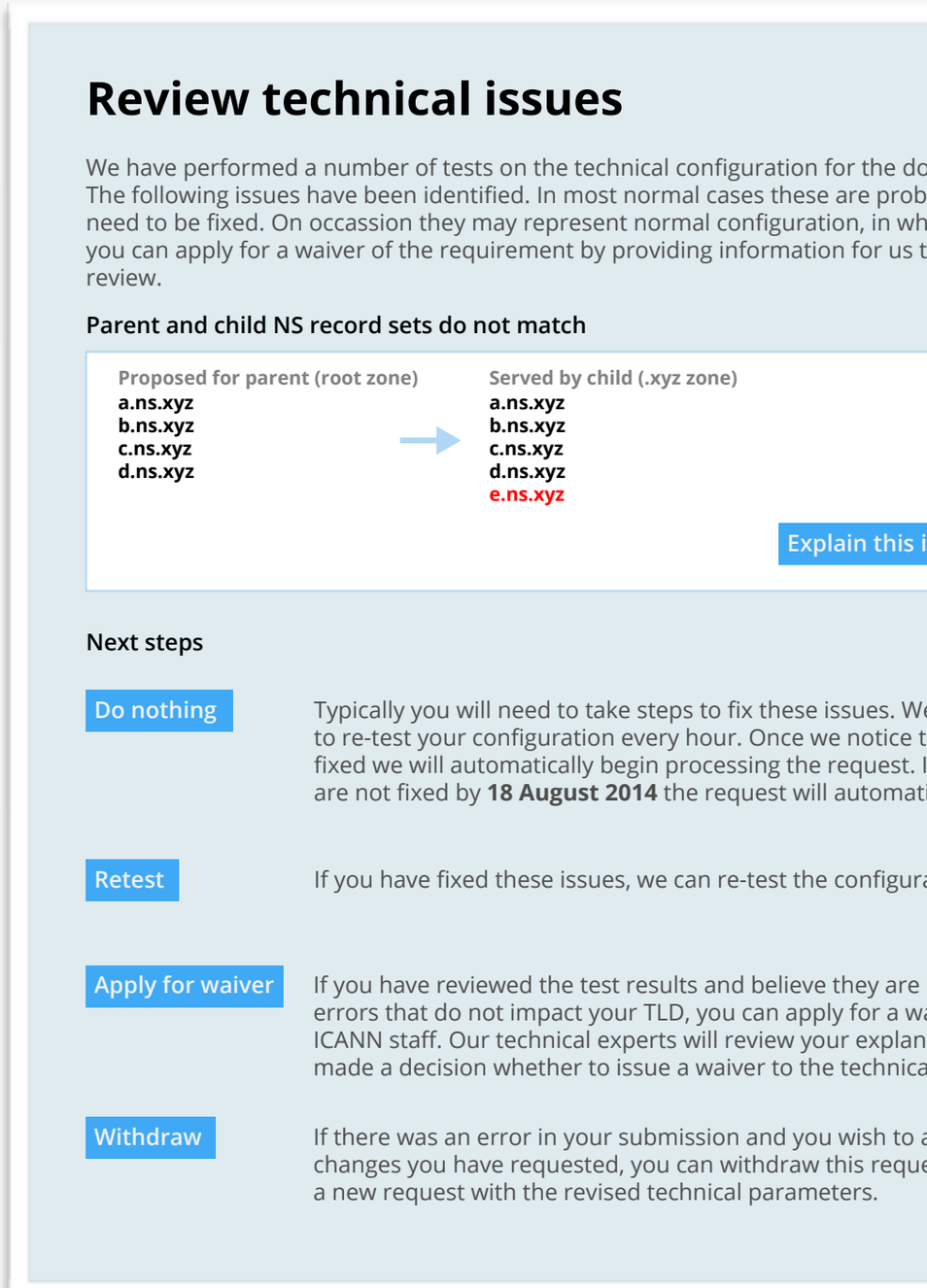
1. Listed in public WHOIS
2. Approves change requests

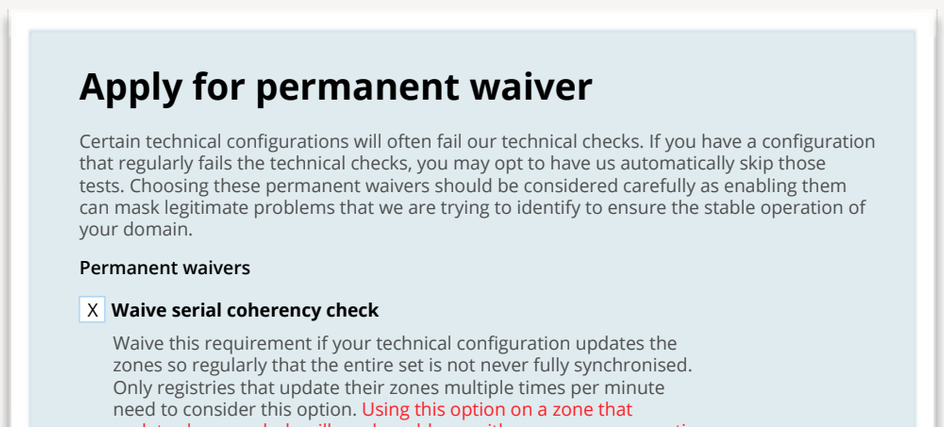
New authorization model



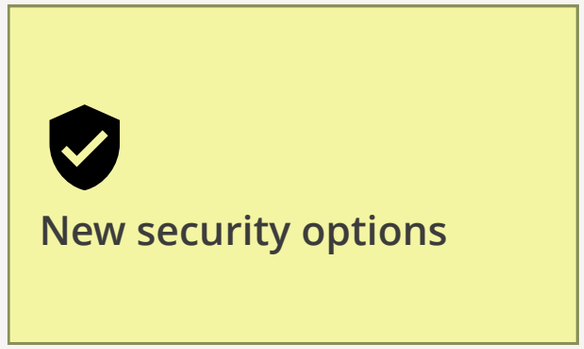
New technical check implementation

- Separating the technical check processes into a separate system.
- Can be maintained independently of the RZMS.
- Published openly.
- Richer reporting and analysis.
- Comprehensive debugging logs kept for each test run, customers can view using self-service mechanisms.
- Better parallelism to address potential delays in current approach.
- Capability for recurring, minor issues to be marked as waivable.





- Provide a mechanism for customers to interact with RZMS programmatically (using tools rather than manually interacting with website).
- Removes error-prone steps for customers with large portfolios
- Provides easy mechanism to perform bulk operations (submissions, status checking, etc.)



- Add two-factor authentication capability
- Migrate from role accounts to person based accounts
- Eliminate email-based submission
- Comprehensive audit trail available to customers to see who did exactly what, when.

FOI implementation

- Implement terminology changes associated with FOI recommendations (e.g. phase out “redelegation”, “sponsoring organization”, etc.)
- Implement process changes associated with redelegation process.
  - “delegation contact”

Feedback welcome.