Technical Check Evolution

ICANN DNS Symposium
November 2022

Kim Davies
VP, IANA Services, ICANN
President, PTI

PTI | An ICANN Affiliate

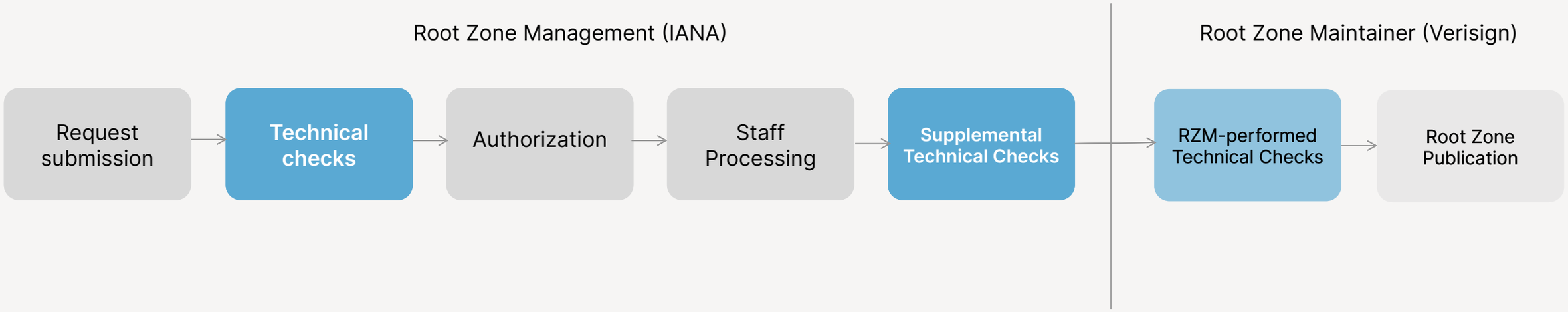
Agenda

- IANA's current processes
- Evolution of our root zone management system
- Ideas for evolving technical checks
- Next steps

Current process

- Set of tests performed when evaluating change requests for the DNS root zone (i.e. for TLD delegations)
- Largely the result of a 2007 consultation
  - Additional tests added in 2010 for DNSSEC
- Not intended to check for all best practices
- Serves as important safeguard that change is authentic
  - Part of the test suite matches proposed changes with contents of child zone

Typical request workflow

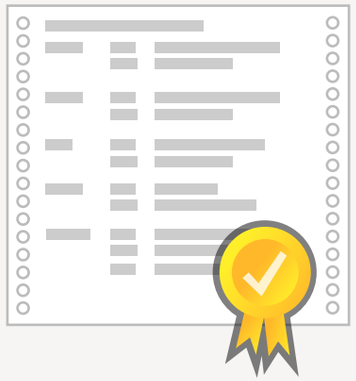


Root Zone Distribution

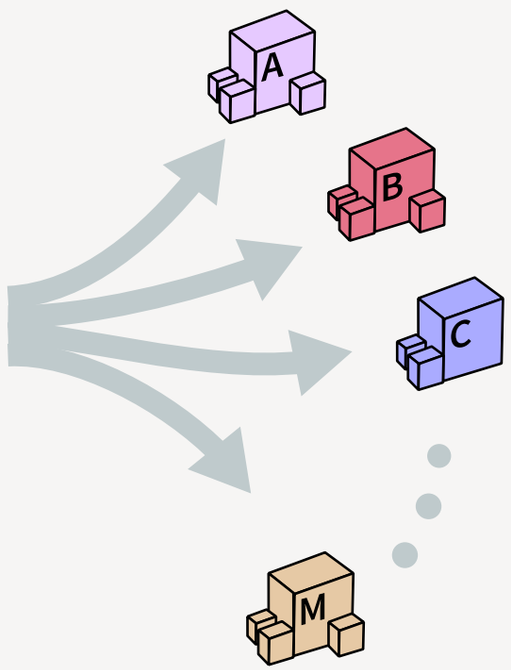
Production

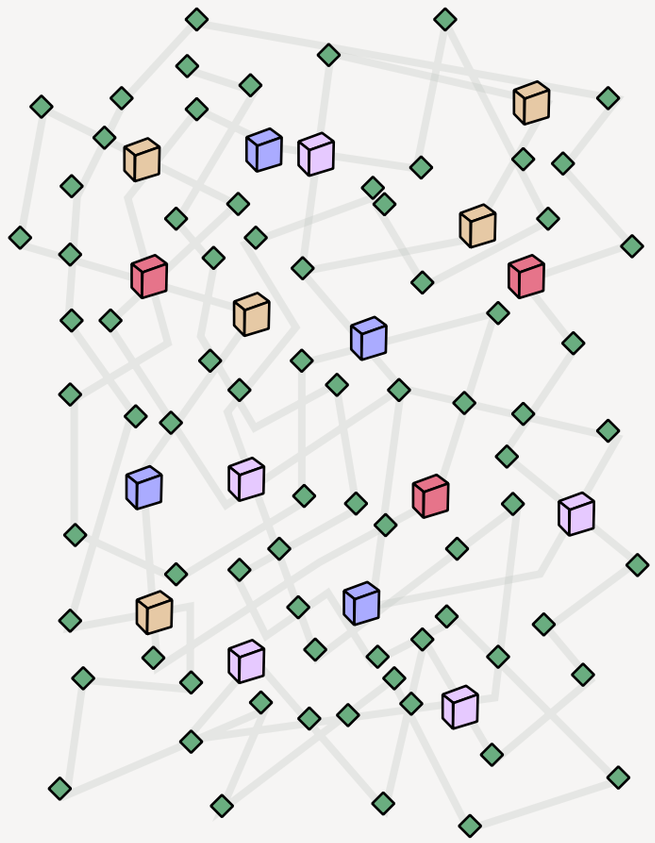
Distribution

Root Zone Database

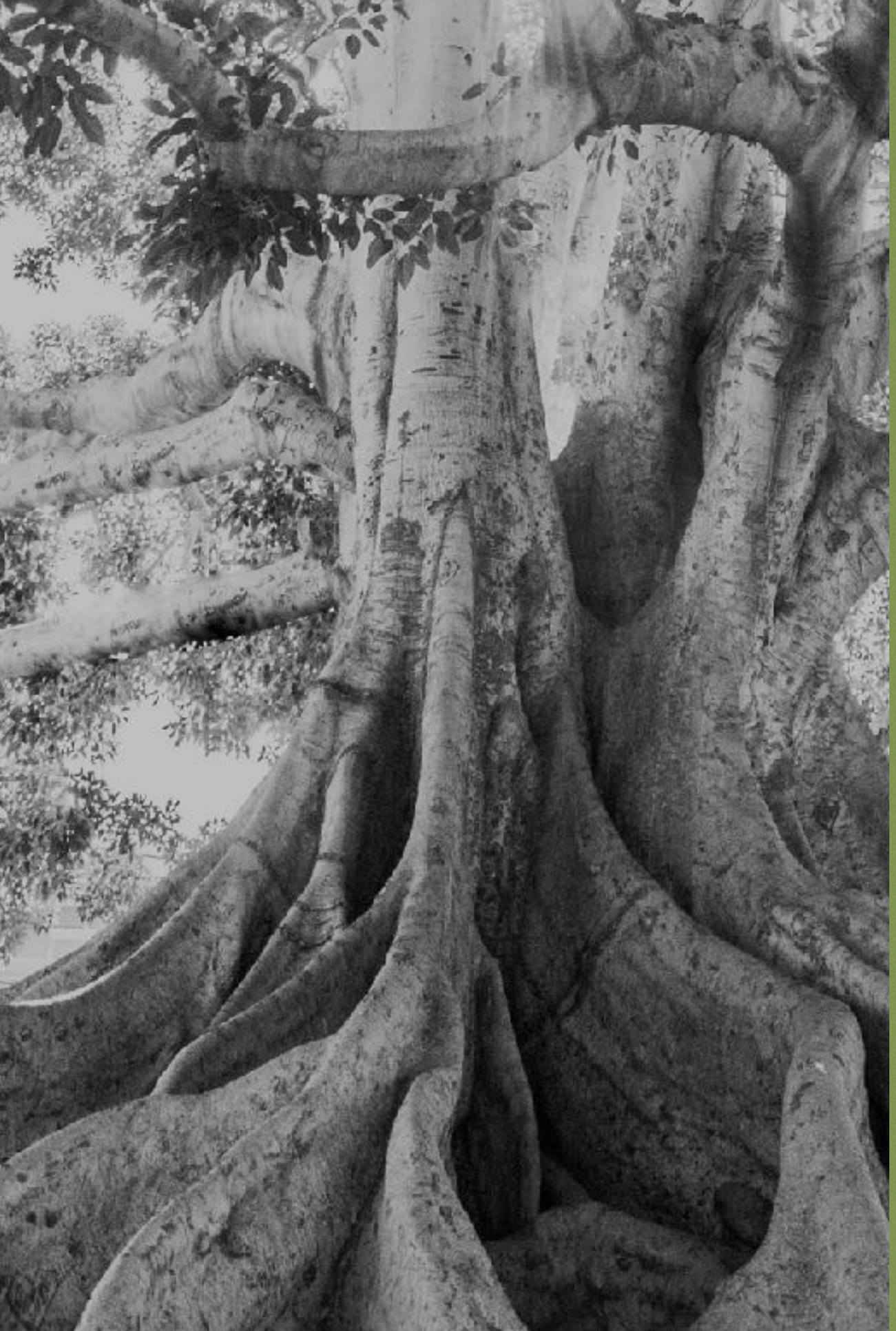


Root Zone File





Root Servers



Current test regimen

Current DNS tests

- **Minimum number of nameservers**
  - At least 2 NS records
  - Must not have matching IP addresses
- **Valid hostnames**
  - Comply with RFC 1123 s2.1 (i.e. LDH)
  - IDN U-labels not permitted (A-labels OK)
- **Name server reachability**
  - Both TCP and UDP required
- **Authoritative**
  - AA-bit set in response to query with no RD-bit

Current DNS tests

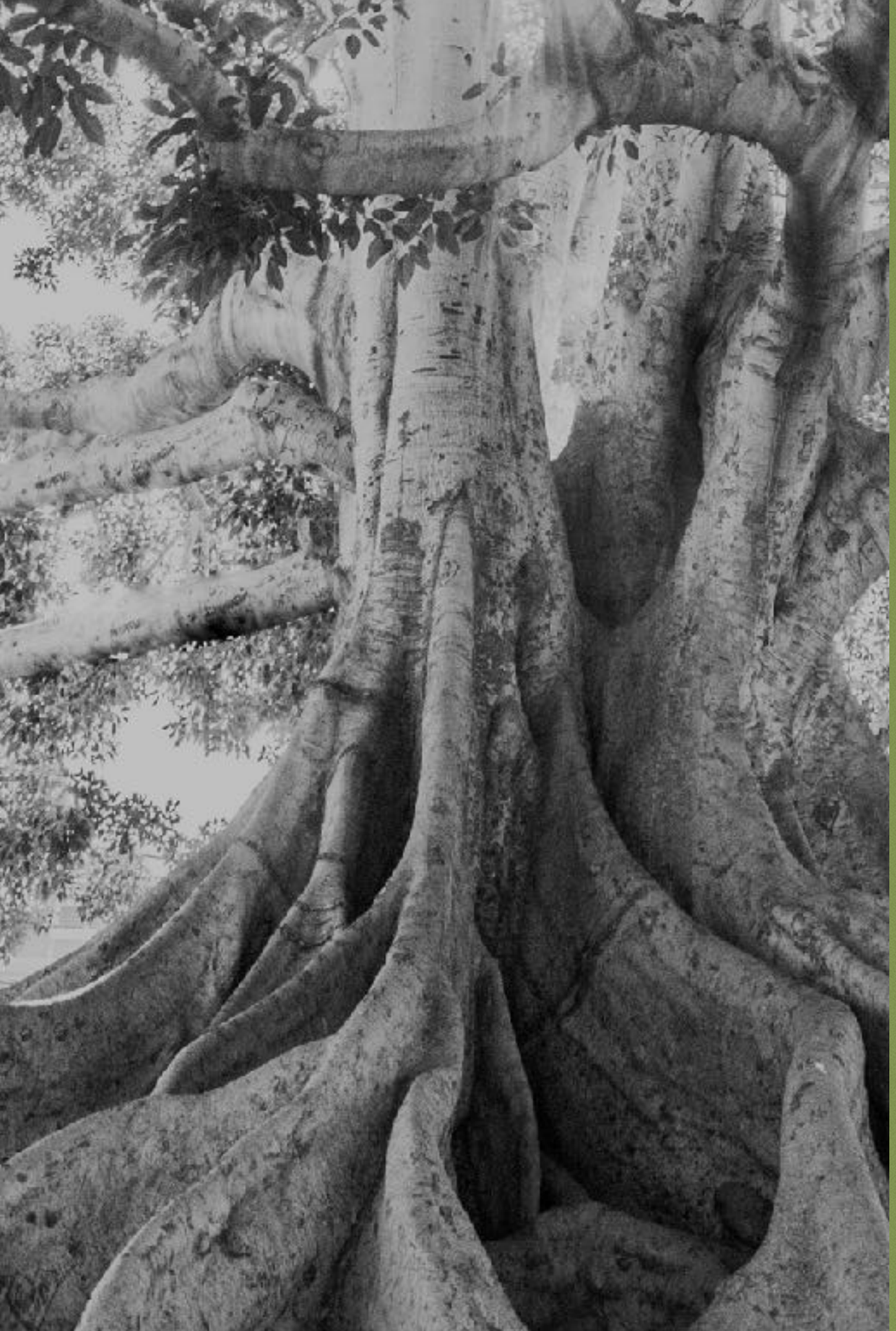
- **Network diversity**
  - No common origin AS across the set (for each transport type)
- **Glue consistency**
  - Proposed glue records for root zone must match A/AAAA records of host
- **Delegation consistency**
  - Proposed NS-set for delegation must match apex NS-set for child
- **Consistency between name servers**
  - Each authoritative nameserver should serve consistent data
  - Currently tests for NS-set and SOA (i.e. serial number)

Current DNS tests

- **No truncation of referrals**
  - Entire NS-set plus minimal glue needs to fix in 512-byte
- **Prohibited networks**
  - No use of special-use IP addresses for nameservers
- **DS records have matching DNSKEY**
  - Don’t need to be signed using each DNSKEY
- **SOA can be validated with the DS set**

Current RDDS tests

- **WHOIS protocol**
  - Basic connectivity test to TCP port 43
- **RDAP protocol**
  - Well-formed URL
  - Returns appropriate status code (2xx/4xx)
  - If a domain object is returned, well-formed
  - If is a redirect, the redirect target must conform



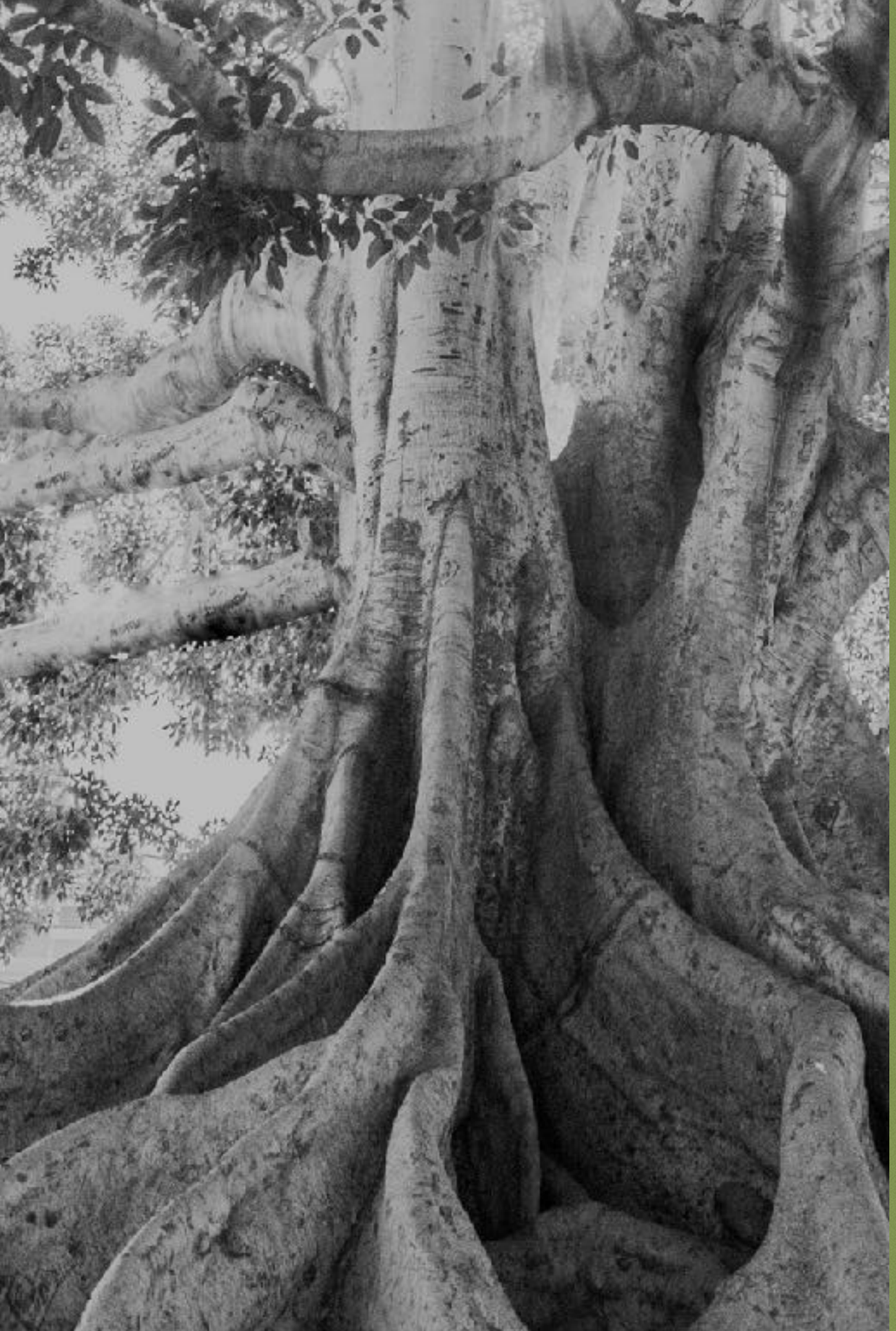
Experience with the current tests

Some experience with current tests

- **False negatives for zone coherency**
  - Particularly for rapidly fluctuating zone content
- **RSP changes**
  - Significant (i.e. wholesale) changes to registry backend require multi-step process for key rollover and NS transition
    - NS changes are recommended to be multi-step
- **Standby keys**
  - Generating an additional key, often kept offline, to facilitate a quick rollover within the child
  - Some operators unwilling to publish its respective private key in the zone apex prior to use

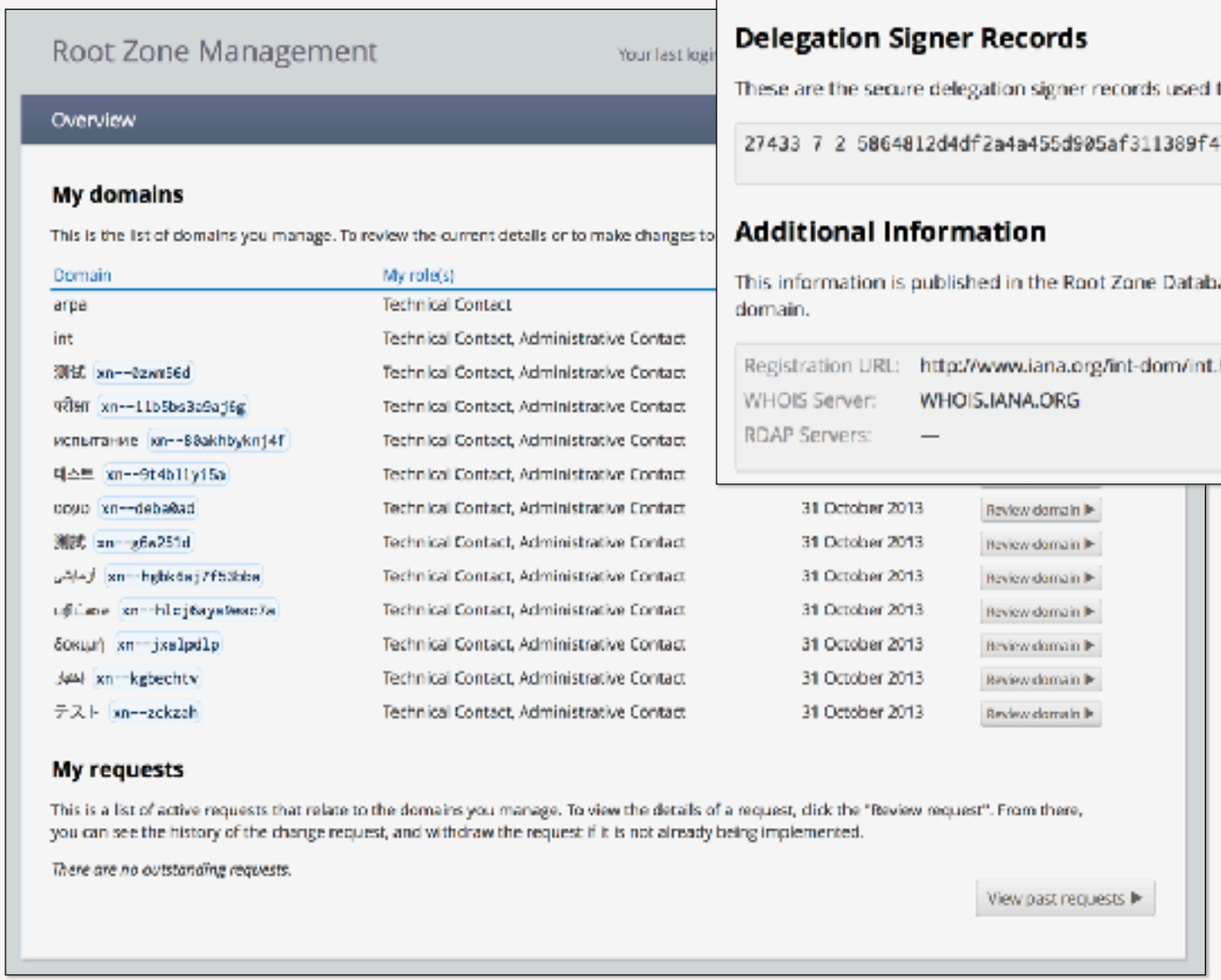
Some experience with current tests

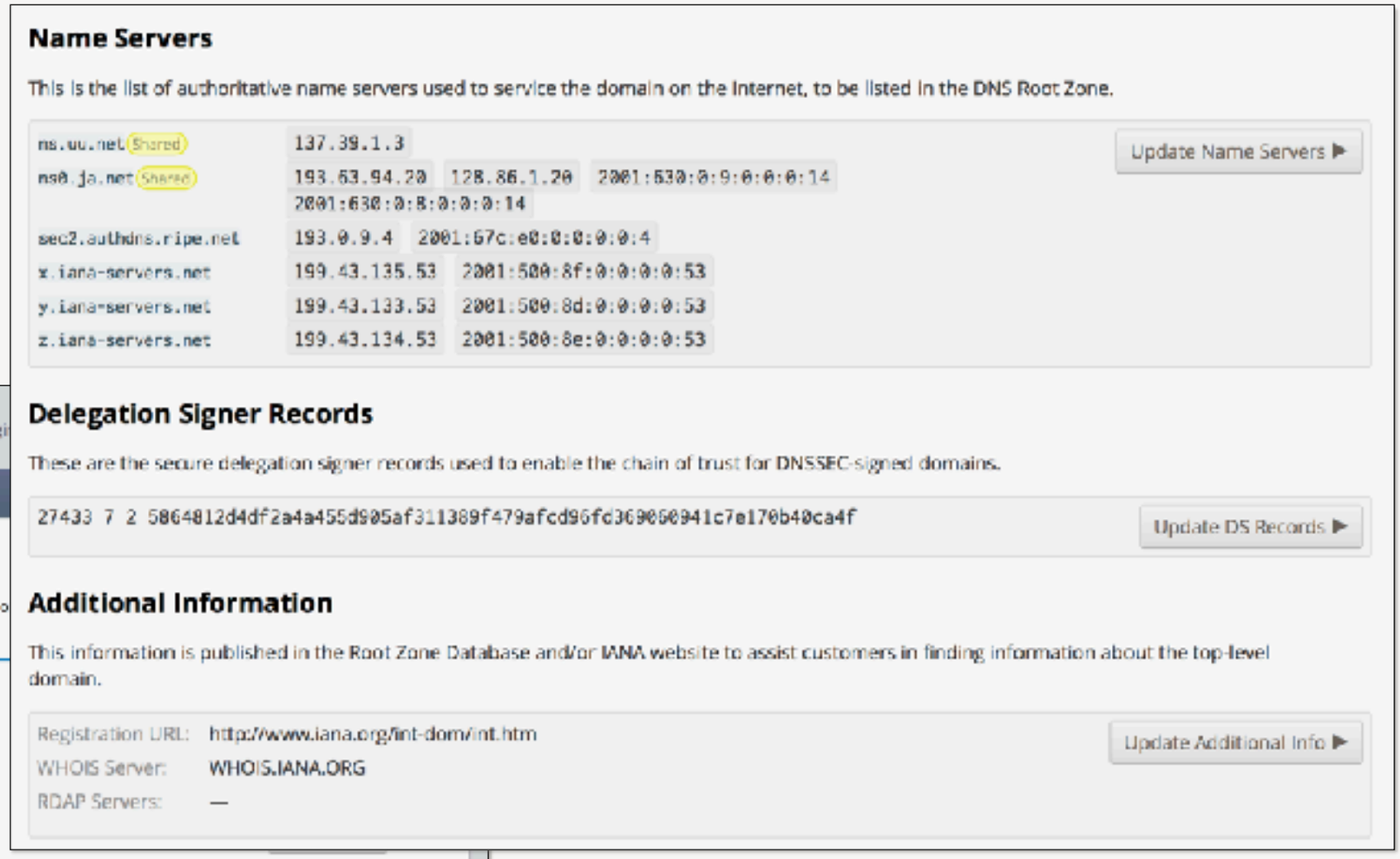
- **Network diversity**
  - Some operators want a single vendor to operate all infrastructure
  - Some RSPs have stood up second AS to fulfil IANA requirement



Our evolving root zone management platform

Customers typically interact through the RZMS

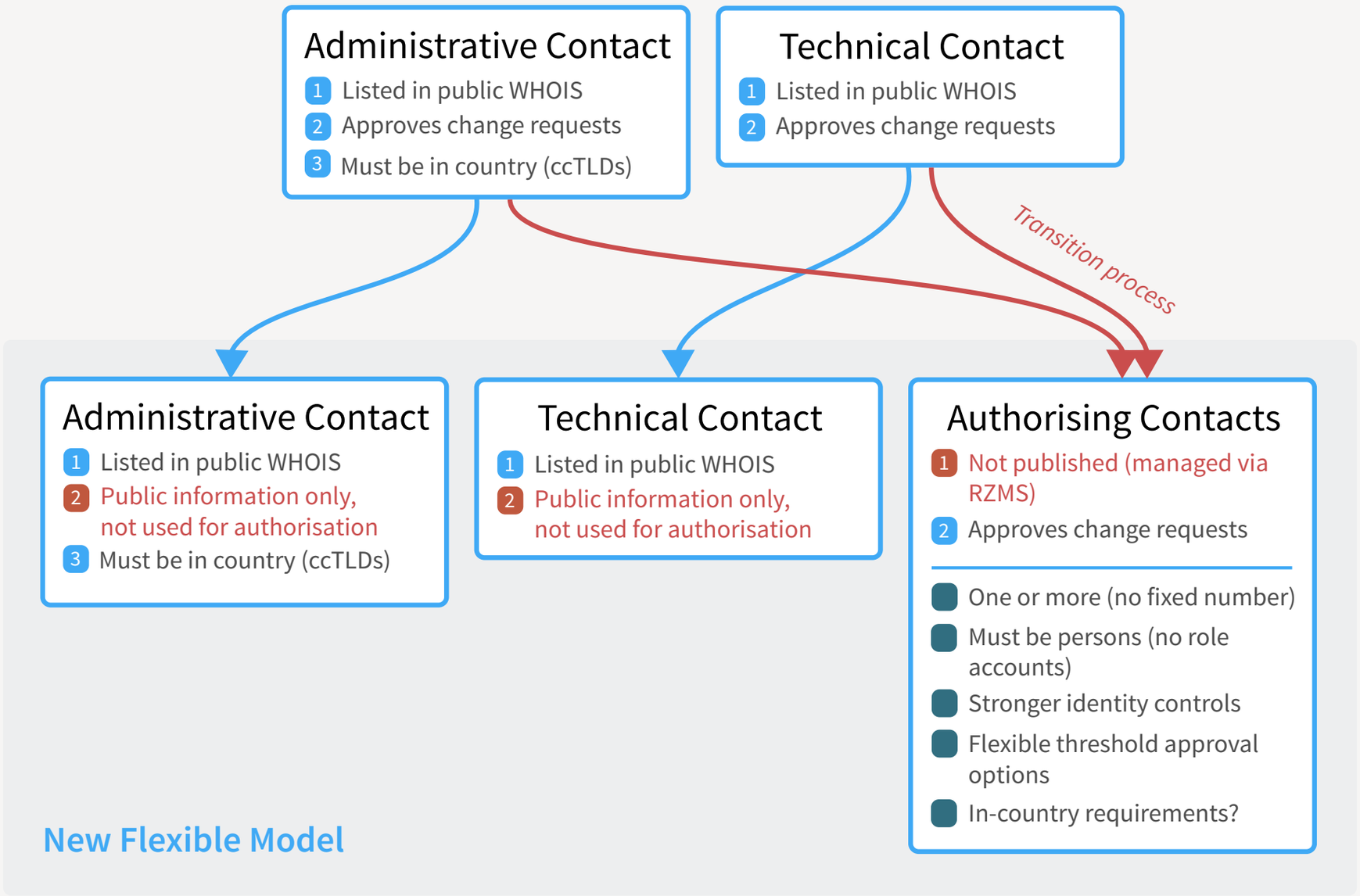




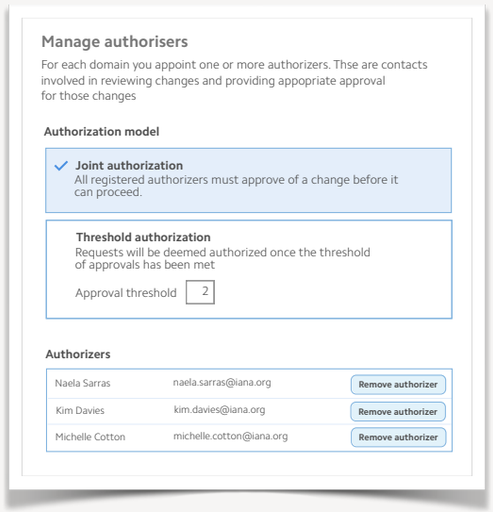
- Root Zone Management System (RZMS) provides self-service capabilities
- Significant next-gen update coming soon

Next-gen focus areas

New authorization model. Separation between public points of contact and users who can submit and authorize requests.



Next-gen focus areas



Approval thresholds. Decide how many contacts must approve changes (1, 2, 3 or more, or all.)

Granularity. Authorizers can be configured to be (technical, not-technical, transfers etc.)

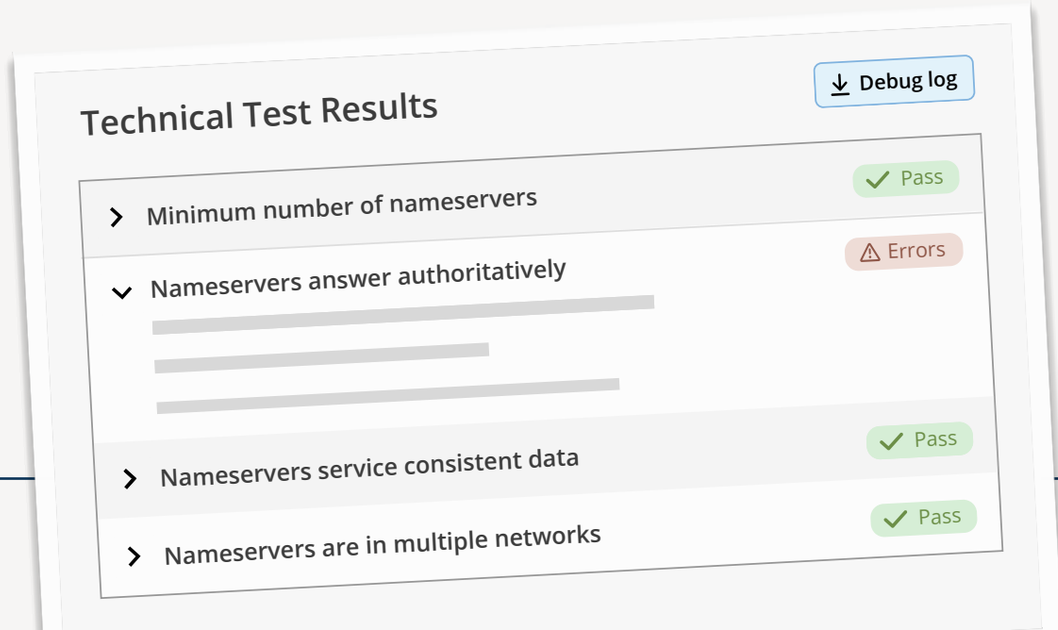
Security. Improved techniques like audit logs and multi-factor authentication.

```
tlds = ['example', 'foo', 'آزمایشی']
for tld in tlds:
    payload = {
        "domain": tld,
        "changes": {
            "rdap_server": "rdap.nic.{}".format(tld)
        }
    }
    url = "https://beta.api.rzm.iana.org/submit-change"
    requests.post(url, json=payload)
```

Automation. Development of APIs and other tools to help automate and manage large portfolios.

Next-gen focus areas

- **Technical check system**
  - A new standalone service 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
    - Self-service
  - Richer explanations that should be more intuitive
  - Does not change the test definitions (yet..)

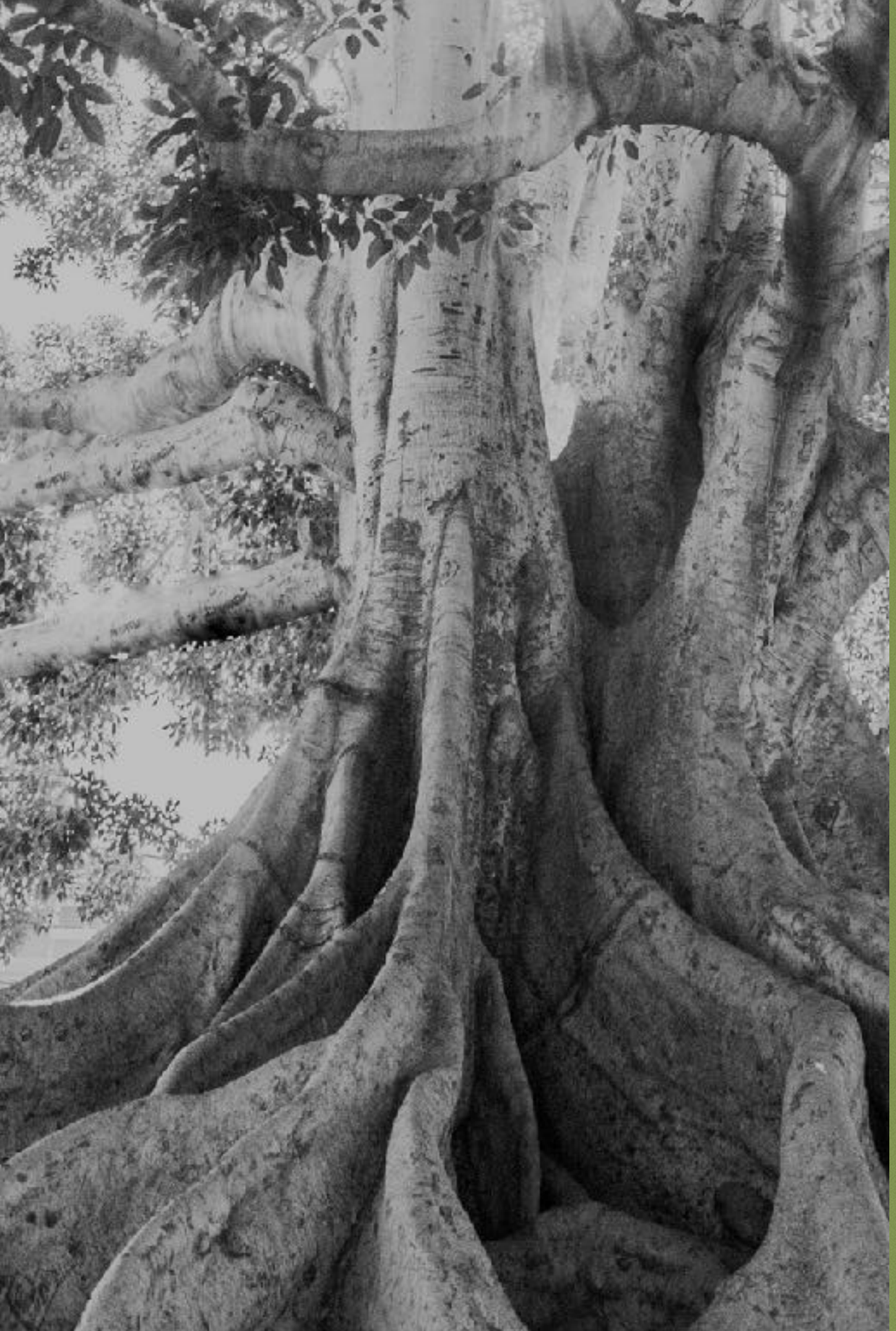


Next-gen focus areas

- **Adding a “warn” classification for less severe issues**
  - The current system is a “pass/fail” system
    - If all tests pass, moves to the next processing phase automatically
    - If any tests fail, returned to the customer for cure
      - Customer may ask for a waiver if they feel test is erroneous
      - Manual process, staff discretion
  - Adding a new “warn” category, i.e. “pass/warn/fail”
    - Issues identified that are less severe
    - Provide self-service capability for the customer to self-dismiss
    - No IANA staff involvement (customer can always ask questions)

Root Zone Update Study

- ICANN commissioned a study on how root zone update process could be improved, outcome of the 2016 IANA stewardship transition
- Involved interviews with customers and detailed review of existing processes by multi-disciplinary independent review team
- The study team, ICJ, found for technical checks:
  - “In the contemplated pass/warn/fail revision to RZMS, ICJ supports making serial number inconsistency a non-blocking warning that can be acknowledged and bypassed by TLD operators.”
  - “ICJ recommends IANA consider a recurring “health check” service.”



Evolving how tests are performed

Evolving our operations

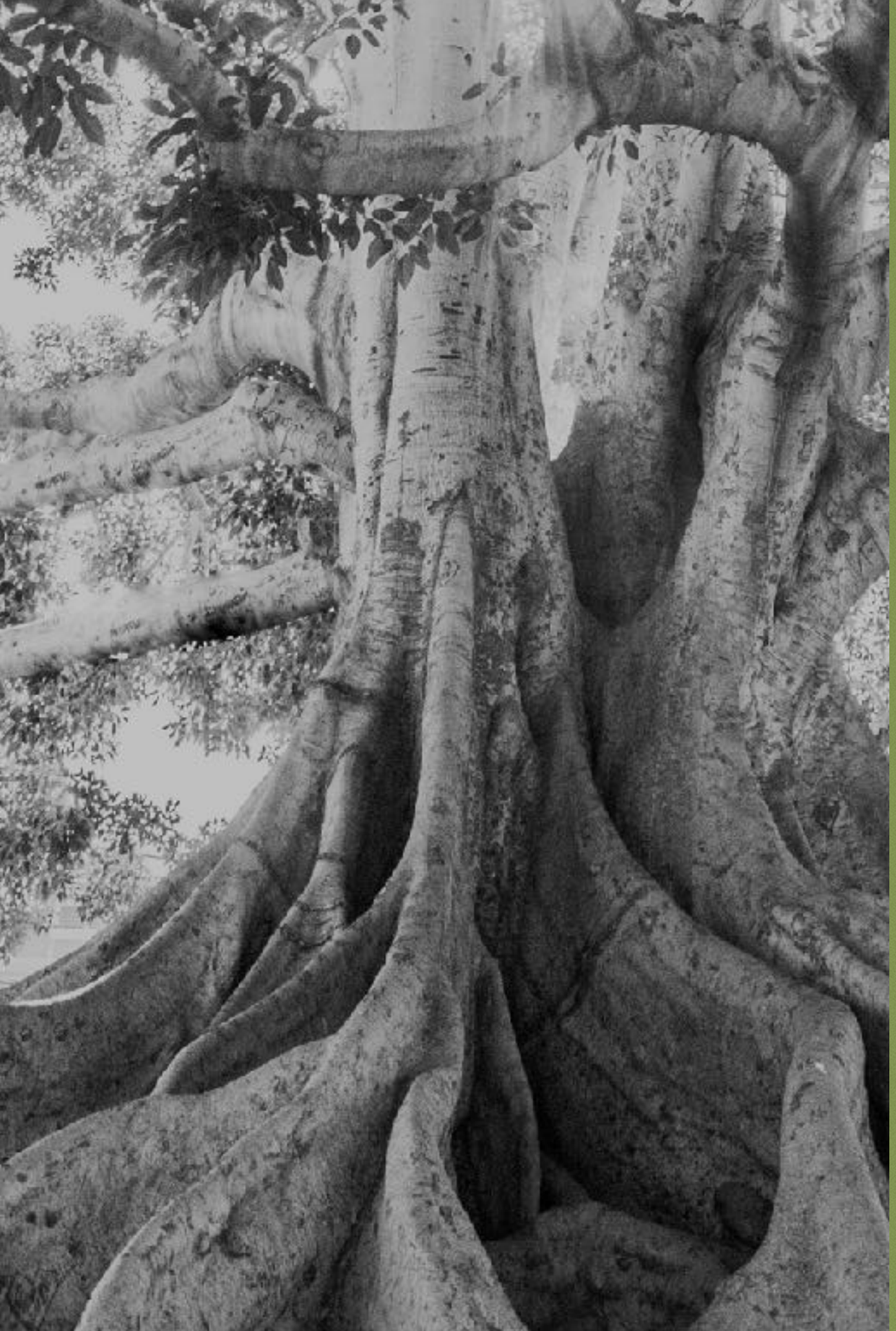
- **Test scope and definition**
  - We believe it is now a good to re-evaluate how we perform conformance testing (“tech check”) for root zone changes.
    - A lot has evolved in the operational environment in 15 years
  - We’ve received general feedback over the years on suggestions from customers for refinement.
  - Root Zone Update Study provided useful inputs
  - 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

- **Proactive testing**
  - Our proposal: proactive regular monitoring of all TLD delegations
  - Expanding upon just child synchronization monitoring
    - Notify of emerging issues more generally
    - Provide actionable triggers, such as drafting a change request, when certain conditions can be detected
    - 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 into a singular view
    - Password/credential aging and/or vulnerability alerts
    - Validate contact methods, age out old unverified ones

Evolving our operations

- **Change to glue consent**
  - Current approach requires approval from **all** impacted TLDs
  - Logistically challenging (although less so over time due to evolving usage patterns)
  - Moving to a new model
    - Approval only required by the submitting TLD
    - Mandatory 14 day objection period where other TLDs may raise concerns with the change, otherwise moves forward by default
  - Increasing prevalence of in-bailiwick names for shared nameserver infrastructure, renders these issues moot



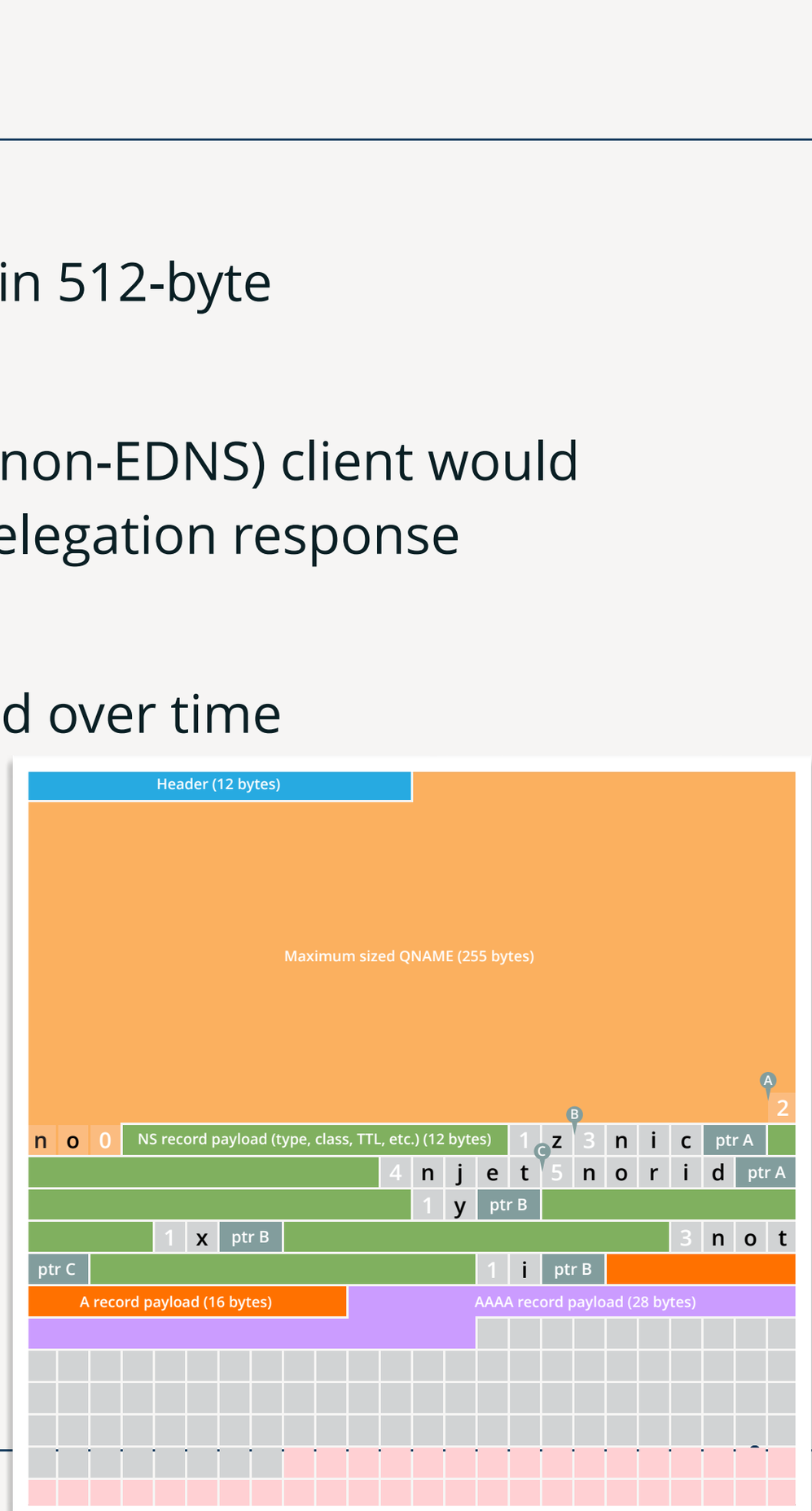
Evolving how tests are defined

Preamble

- Non-exhaustive set of possible refinements
  - Not intended to be definitive recommendations
- Some collected from customer feedback
- Some based on staff experience

Re-evaluating size requirements

- Entire NS-set plus minimal glue needs to fit in 512-byte
  - (1 A and 1 AAAA)
- Rooted in the assumption that a legacy (i.e. non-EDNS) client would default to TCP if this was exceeded by the delegation response
  - Is this still a useful assumption?
- Demand for relaxing requirement has waned over time



Role of supplemental technical check

- Currently tests are re-performed by IANA prior to transmission to the root zone maintainer
- Safeguard against a deterioration of a TLD's configuration while processing has been conducted
- Derives from an era where the process was slower
- Opportunity to eliminate this phase, or only trigger when a certain time has elapsed since last successful test?
- If retained, capture the basis for any waivers and apply them

Clarifying TLS validation

- For RDAP, testing has relied on default local trust stores for acceptable CA roots (i.e. from our library implementation)
- Unclear what expectations should be set for the provenance of certificates used for RDAP servers
- Would likely benefit from being more explicit

Algorithm selection

- Root zone permits a subset of algorithms and digest types
  - DSA/SHA-1 (3), RSA/SHA-1 (5), DSA/SHA-1/NSEC3 (6), DSA/SHA-1/NSEC3 (7), RSA/SHA-256 (8), RSA/SHA-512 (10), ECC-GOST (12), ECDSA P-256/SHA-256 (13), ECDSA P-384/SHA-384 (14)
    - Not: EdDSA 25519 (15), EdDSA 448 (16)
  - SHA-1 (1), SHA-256 (2), GOST (3), SHA-384 (4)
    - All
- New algorithms agrees between root zone partners after demonstration of mature implementations and well-tested in other zones
- Removing algorithm support
  - No formal procedure
  - Should IANA have a role in phasing out older algorithms and digest types? Is there any circumstance it should be proactive?
  - Sunset date or just not allow new records?
- DNSSEC algorithm priority

Child key rollovers

- IANA requires DS records to be demonstrated in the child zone with a DNSKEY record
  - No need to sign with all of the keys, but their public key must be present at the apex
  - Forms an important validation step to ensure the party with editorial control of the zone is requesting the change
    - See discussion in Root Zone Update study
    - Powerful validation against errors
- A small subset of operators request adding DS records with no proof in the child zone
  - Some argue not consistent with “Double-DS” method in RFC 7583 s3.3.2
  - Several TLDs have gone bogus after asking to skip this test, taking the new DS on faith, and then performing a rollover to the wrong key

Going insecure

- There is no special business logic today for “going insecure” — removing all DS records from the delegation
- Removing them does have consequences
  - Instant contractual breach for most TLDs
  - Relying parties that may expect DNSSEC downstream will no longer be secure (DANE, etc.).
- Even as a courtesy, may make sense to gate such changes with additional confirmation logic to avoid surprises

Regular Monitoring

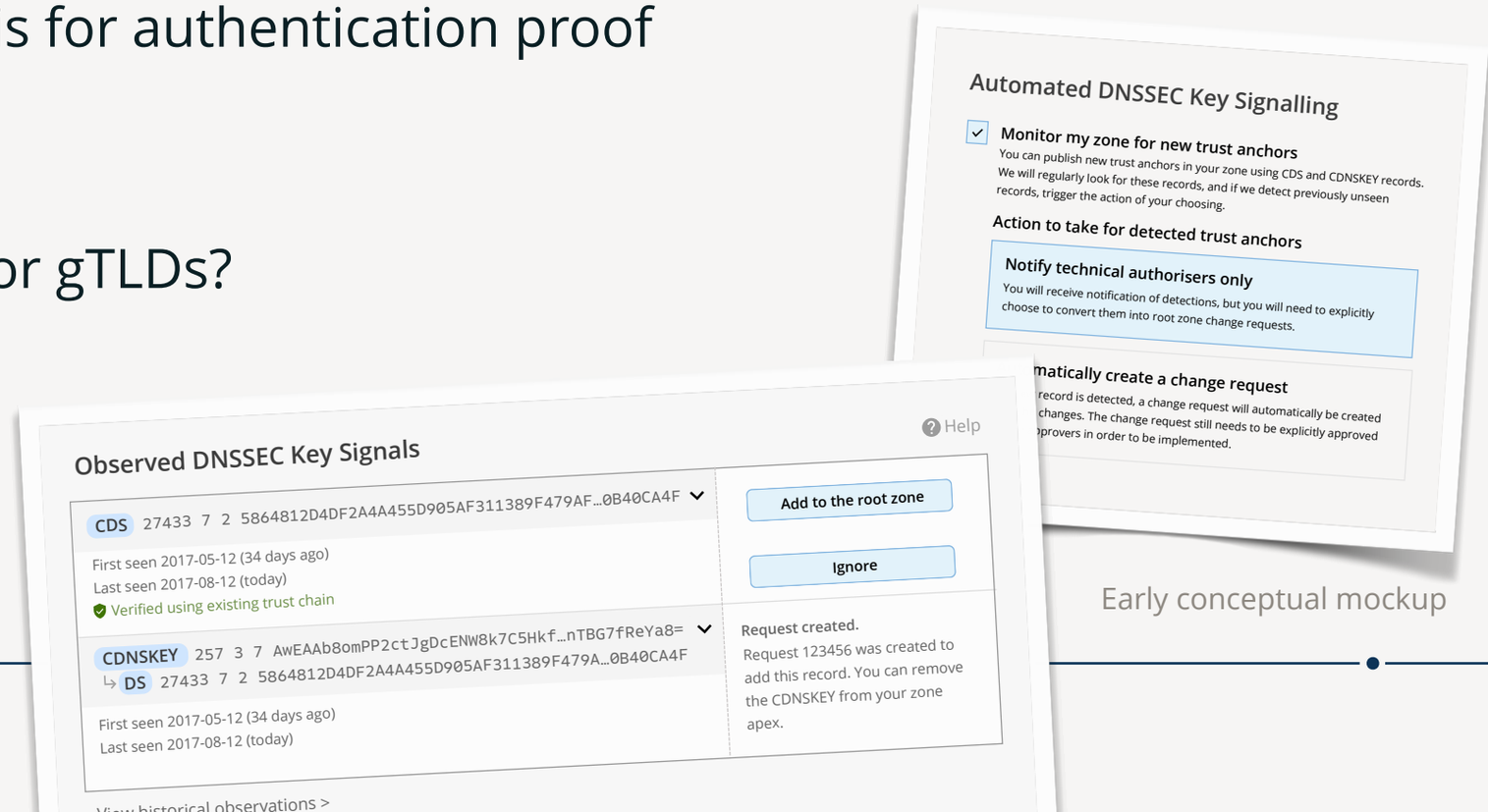
- Current tests only performed during change request
- Can we identify emerging issues without waiting for the next change request?
- Anticipate moving to a model where tests are regularly conducted
  - Notify customer of new variances
  - Provide ‘one-click’ capability to trigger corrective changes
  - Form part of a overall ‘health check’ provided to TLD managers
- Same polling mechanism could monitor for CDS/CDNSKEY/CSYNC signals
- Consider overlap with ICANN SLA monitoring for gTLDs

Child signals for delegation changes

- CDS/CDNSKEY provide a way for child zone to signal changes to their DS records in the parent
- CSYNC provide similar mechanism for NS changes

- Been on our backlog for many years, first interest from TLD managers earlier this year.
- Due to criticality of the root zone, unlikely to be a conventional implementation
  - Triggers could pre-populate and start a change request
  - Same authorizations etc. would still be required
- Could serve as an alternative basis for authentication proof (i.e. CDNSKEY instead of DNSKEY)

- Contractual changes to support for gTLDs?



Early conceptual mockup

Testing from multiple vantage points

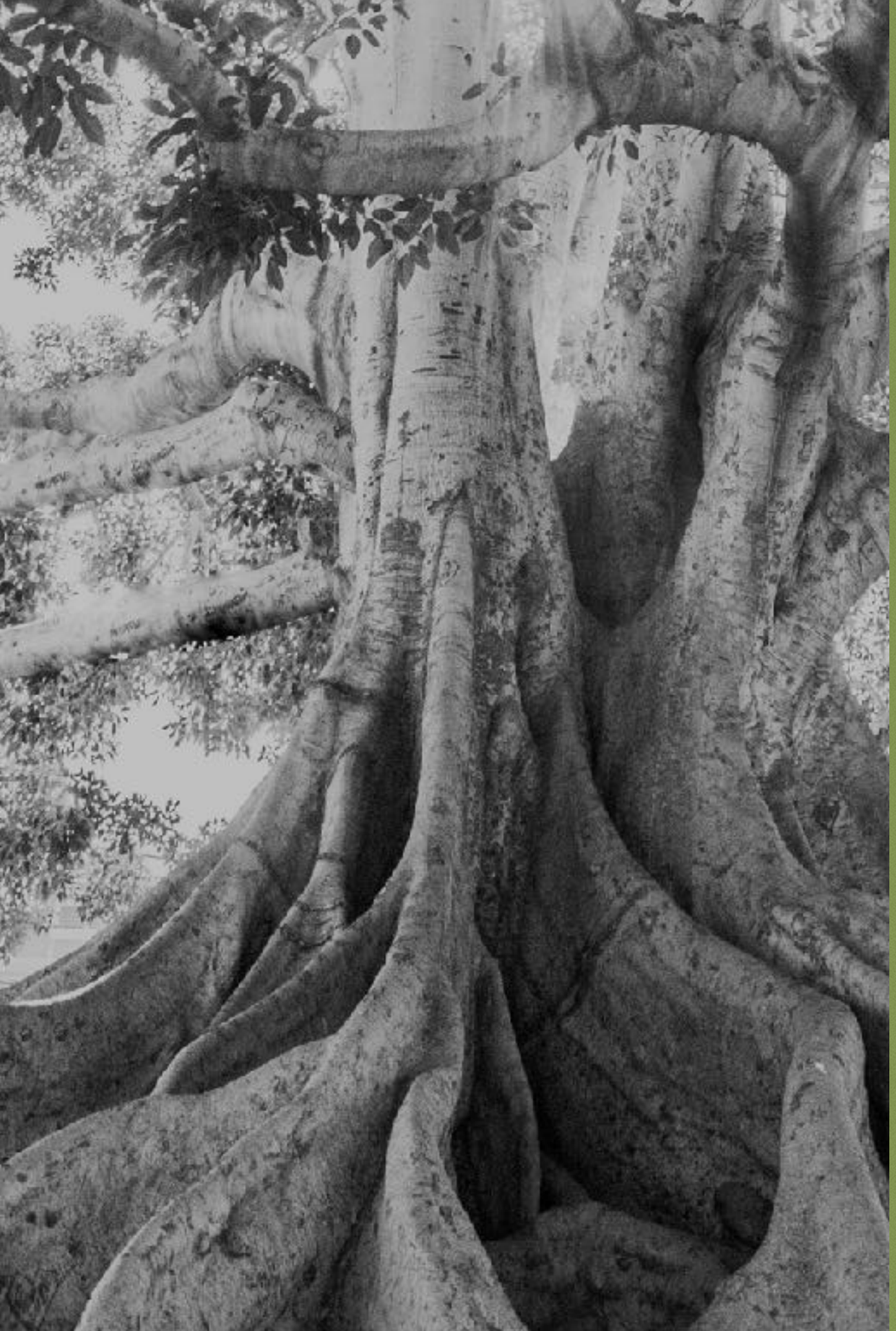
- Currently, tests are performed from ICANN's active site in an active/passive configuration.
  - If there are checks that fail, staff have the ability to execute tests from alternate locations
- May benefit from multiple test locations as the norm, rather than by exception
- IANA could expand its test sites, and could operate the suite in parallel through the new modular framework
  - Performance: may incur a penalty, may be faster, depending on consensus approach
- However, they may be even greater utility leveraging third party resolvers
  - Truer indication of "real-world" view (albeit more likely cached)
  - Less likely to be subject to rate limiting (increasing problem for IANA)

Other suggested test areas

- **NSEC3 parameter settings**
  - Warn or error if iteration count too high
- **Algorithm quality**
- **More protocol compliance**
  - Case preservation
  - EDNS capabilities
- **SEP-bit**
  - Sometimes operators point to a ZSK
  - It still works, and one RSP explicitly wanted this configuration
  - But nonetheless a lack of SEP-bit is probably indicative of a problem

Other issues

- Nameserver operator wants to be removed from delegation but TLD manager is unresponsive
- Nameserver is known lame for extended period
- Wholesale nameserver changes
- Active quality monitoring of TLD POCs
  - Periodic email revalidation, phone verification and the like
  - Currently informal processes (annual postal mail campaigns) with manual follow up
- Highly shared infrastructure
  - In light of talks on Tuesday, flagging high-concentration may help manager make informed decisions on diversity



Next steps

What's next?

- Discussion paper lays out these topics
  - What tests suit the current operating environment?
  - With the new ability to 'warn', as well as regular monitoring, are there new things we should consider?

- Outcome of this consultation will inform our future development
  - **Actual implementation subject to resourcing and prioritization**
  - Feedback is welcome on prioritization too

Thank you!

kim.davies@iana.org