Technical Check Evolution

ICANN DNS Symposium November 2022

Kim Davies VP, IANA Services, ICANN President, PTI

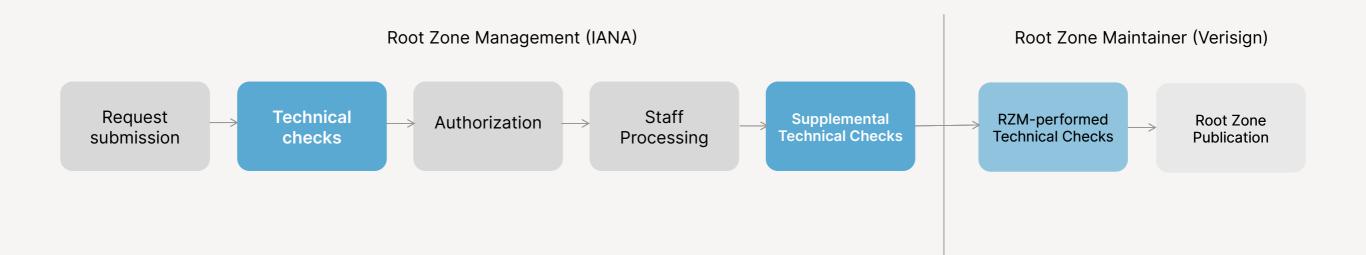
PTI | An ICANN Affiliate



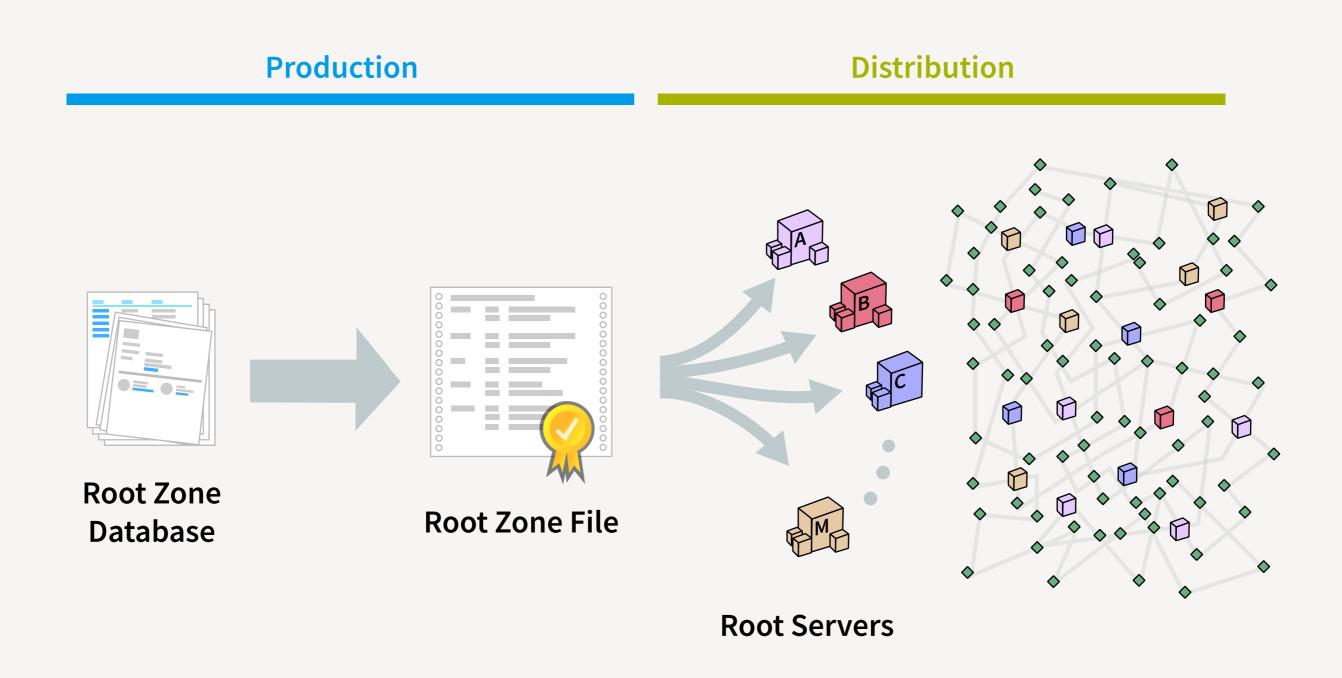
Agenda

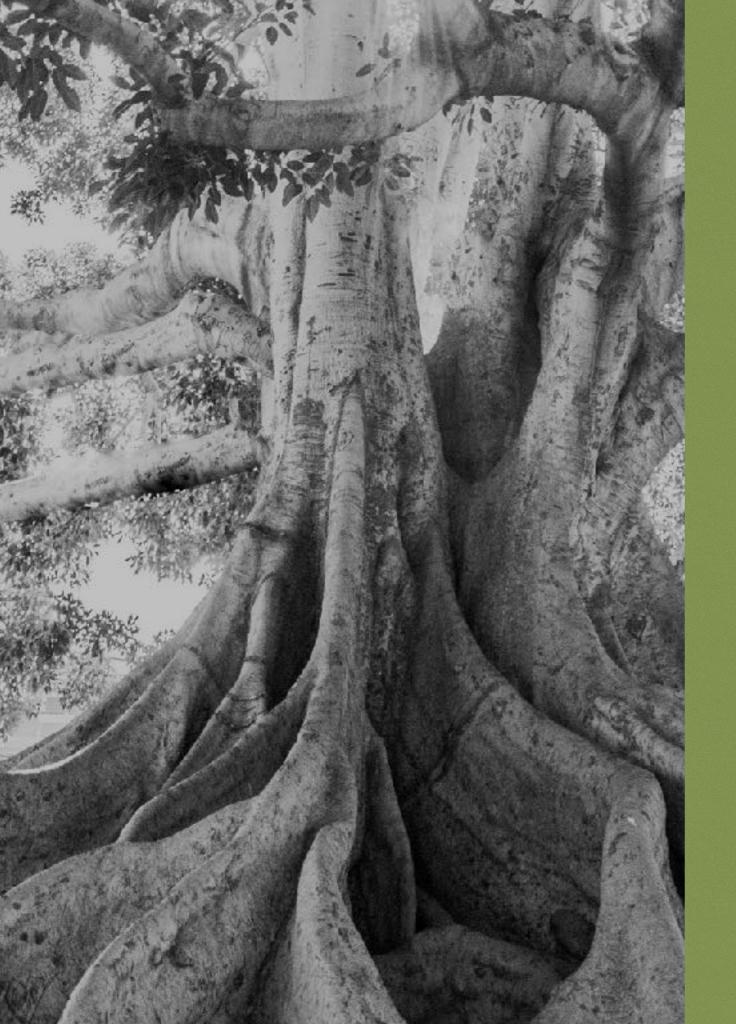
- IANA's current processes
- Evolution of our root zone management system
- Ideas for evolving technical checks
- Next steps

- 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



PTI | An ICANN Affiliate





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

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)

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 multistep 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

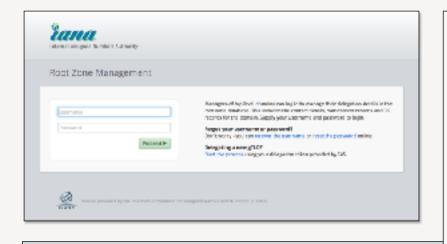
Network diversity

- 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



Name Servers

This is the list of authoritative name servers used to service the domain on the Internet, to be listed in the DNS Root Zone.

ns.uu.net(Shared)	137.39.1.3
ns@.ja.net(Sharee)	193.53.94.20 128.86.1.20 2001:530:0:9:0:0:0:14 2001:630:0:8:0:0:0:14
sec2.authdns.ripe.net	193.0.9.4 2001:67c:e0:0:0:0:0:4
x.iana-servers.net	199.43.135.53 2001:580:8f:0:0:0:0:53
y.iana-servers.net	199.43.133.53 2001:500:8d:0:0:0:0:53
z.iana-servers.net	199.43.134.53 2001:500:8e:0:0:0:0:53

Delegation Signer Records

These are the secure delegation signer records used to enable the chain of trust for DNSSEC-signed domains.

27433 7 2 5864812d4df2a4a455d905af311389f479afcd96fd369050941c7e170b40ca4f

Overview

My domains

Root Zone Management

This is the list of domains you manage. To review the current details or to make changes to		Additional Information			
Domain	My role(s)	This information is published in the Root Zone Database and/or IANA website to assist customers in finding information about the top-level			
arpa	Technical Contact	domain.			
int	Technical Contact, Administrative Contact				
测试 xn0zwn56d	Technical Contact, Administrative Contact	Registration URL: http://www.iana.org/int-dom/int.htm Update Additional Info ►			
परीक्षा xn11b5bs3a6aj6g	Technical Contact, Administrative Contact	WHOIS Server: WHOIS.IANA.ORG			
испытание м88akhbyknj4f	Technical Contact, Administrative Contact	RDAP Servers: -			
텍스트 xn9t4b11y15a	Technical Contact, Administrative Contact				
0090 xndeba0ad	Technical Contact, Administrative Contact	31 October 2013 Review domain ►			
测试 ang6w251d	Technical Contact, Administrative Contact	31 October 2013 Review domain 🕨			
$_{\omega} \Delta (aj = j / a)$	Technical Contact, Administrative Contact	31 October 2013 Review durnalle Root Zone Management			
uffilme xn-hlojtaysDesc7a	Technical Contact, Administrative Contact	31 October 2013 Review domain ►			

Technical Contact, Administrative Contact, 31 October 2013 Review domain ▶ Technical Contact, Administrative Contact 31 October 2013 Beview domain 🕨 Technical Contact, Administrative Contact 31 October 2013 Review domain 🕨 Technical Contact, Administrative Contact, 31 October 2013 Review domain 🕨

Your last log

My requests

SORLUY) xn jxalpdlp

sate an -- kebechty

テスト xn--zckzah

This is a list of active requests that relate to the domains you manage. To view the details of a request, dick the "Beview request". From there, you can see the history of the charge request, and withdraw the request if it is not already being implemented.

There are no outstanding requests.

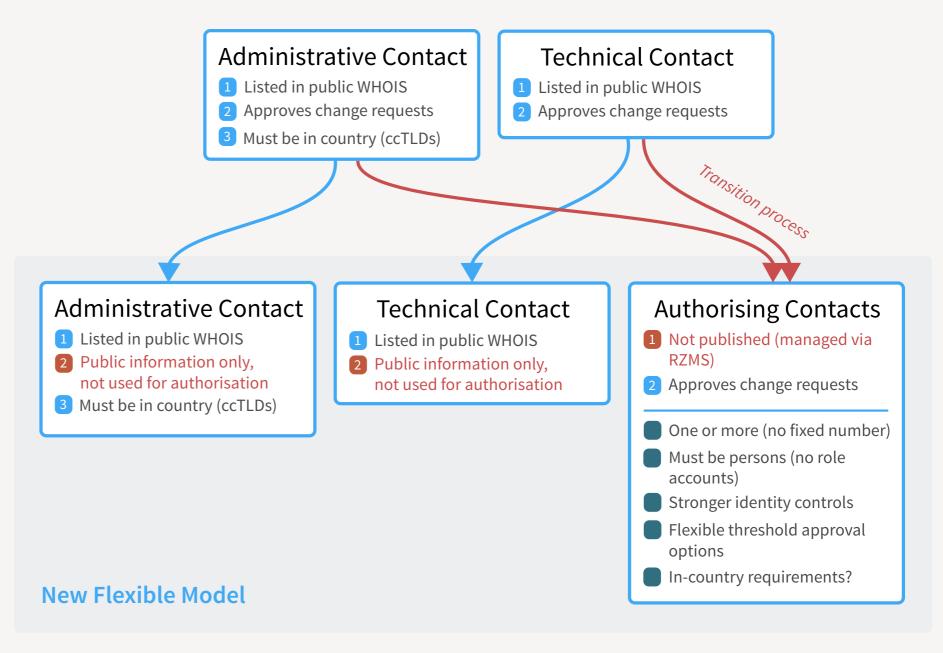
View past requests 🕨

٦t System (RZMS) provides selfservice capabilities

Update DS Records 🕨

Significant next-gen update • coming soon

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



Next-gen focus areas

volved in reviewing r those changes	u appoint one or more authorizers g changes and providing appopria	
uthorization mod	lel	
 Joint authori All registered can proceed. 	ization authorizers must approve of a ch	ange before it
Threshold au Requests will of approvals h Approval thre	be deemed authorized once the t	hreshold
luthorizers		
Naela Sarras	naela.sarras@iana.org	Remove authorizer
	naela.sarras@iana.org kim.davies@iana.org	Remove authorizer

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



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

/ho can authorize trans	lers to this demand
transfer request @prmerly known as a rec new entity. These are considered criticial he ability to approve other kinds of change	delegation) is the transfer of operational control to changes that you may wish to configure differently from e requests. Types
18 CT 78	Mile V. admire
Naela Sarras (naela sarras®iana.org)	
Naela Sarras (naela sarras®iana.org)	Aur (Jampi (Balti). Y
	Are change roads. V Tambes #15
Naela Sarras (naela sarras®iana.org) kim Gavies (kim.davies@iana.org)	Tamakes and the

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



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

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..)

echnical Test Results	
> Minimum number of nameservers	✓ Pass
 Nameservers answer authoritatively 	▲ Errors
i internet data	✓ Pass
Nameservers service consistent data	✓ Pass
> Nameservers are in multiple networks	•

PTI | An ICANN Affiliate

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)

- 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

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

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

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

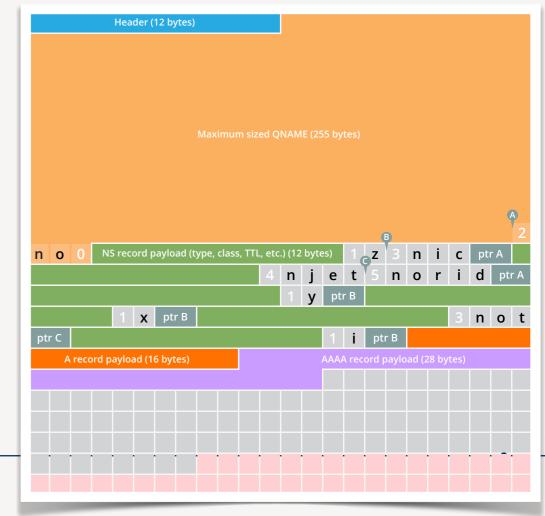


Evolving how tests are defined

Preamble

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

- 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

- 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

- 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

- 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

- 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.

historical observations >

- 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?

PTI | An ICANN Affiliate

Observed DNSSEC Key Signals	🕜 Help	matically create a change request record is detected, a change request will automatically be created changes. The change request still needs to be explicitly approved provers in order to be implemented.	
CDS 27433 7 2 5864812D4DF2A4A455D905AF311389F479AF0B40CA4F ✔	Add to the root zone		
First seen 2017-05-12 (34 days ago) Last seen 2017-08-12 (today) 🥏 Verified using existing trust chain	Ignore	Early conceptual mockup	
CDNSKEY 257 3 7 AwEAAb8omPP2ctJgDcENW8k7C5Hkf…nTBG7fReYa8= → DS 27433 7 2 5864812D4DF2A4A455D905AF311389F479A…0B40CA4F	add this record. You can remove	•	
First seen 2017-05-12 (34 days ago) Last seen 2017-08-12 (today)	the CDNSKEY from your zone apex.		

Automated DNSSEC Key Signalling

Monitor my zone for new trust anchors

ords, trigger the action of your choosing. Action to take for detected trust anchors

Notify technical authorisers only

You will receive notification of detections, but you will need to ex rt them into root zone change requests.

ou can publish new trust anchors in your zone using CDS and CDNSKEY will regularly look for these records, and if we detect previously un

Testing from multiple vantage points

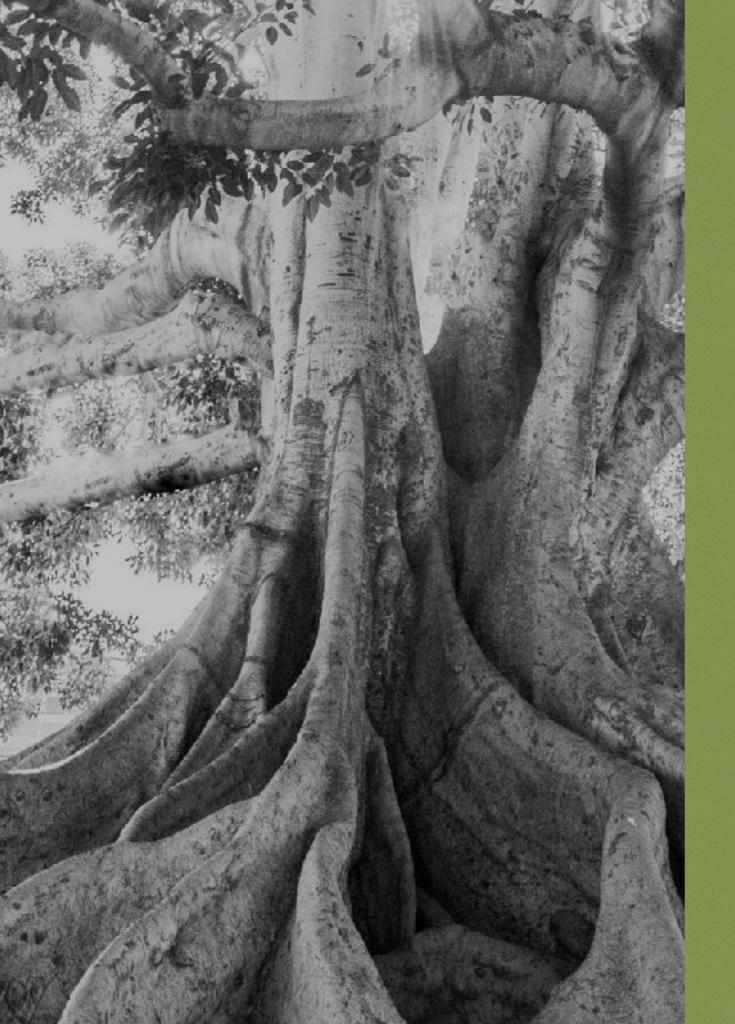
- Currently, tests are performed from ICANN's active site in an active/passive configuration.
 - If there are checks that fail, staff have the ability to execute tests from alternate locations
- May benefit from multiple test locations as the norm, rather than by exception
- IANA could expand its test 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)

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

- 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