Technical topics on the root zone

Kim Davies
IANA Services

APTLD 73: Kathmandu, Nepal
22 February 2018
Common issues at the root zone for TLD delegations
Common issues and how to avoid them

- **Drift of delegation (NS and glue in root) from current configuration**
  - You need to keep the name servers for your domain reflected in your parent (i.e. the root zone)
  - NS set should be the same in your TLD’s zone and the root zone.
  - The IPv4 and IPv6 addresses of your name servers need to be reflected as glue in the root zone.
- Common issue: Adding IPv6 support to a name server and forgetting to update glue.
- Common issue: You need to update the child (authoritative) zone before updating the referral (root zone).
Common issues and how to avoid them

- **Mismatch between DS record and DNSKEYs**
  - When adding delegation signer records to the root zone, there should be a matching DNSKEY (KSK/SEP) in the parent of the child zone.
  - Without this, there is no mechanism to verify the DS record will actually work when put into service.
    - Errors *have* happened.
    - A TLD effectively disappears when there are DS records in the root that do not reflect keys used for signing in a TLD.
Common issues and how to avoid them

- **Lame delegations and unavailable servers**
  - For basic DNS function, the NS set in the root zone need to reflect name servers that are in operation.
  - The root zone should not point to name servers not configured for your TLD ("lame").
  - Develop robust approaches to configuring NS set so it is impervious to outages.
  - Any individual NS may have issues but the whole set should be resilient
  - Techniques like Anycast provide greater resilience
  - Many peers are willing to help.
Common issues and how to avoid them

- **The NS set must fit within a limited packet size**
  - Larger NS sets can not fit within a single UDP packet.
  - Use name server compression to your advantage.
    - e.g. [a-z].ns.[tld]
New initiatives at IANA
New initiatives

• Recently implemented support for elliptic curve cryptography for DNSSEC
• We are implementing a ground up re-write of the Root Zone Management System
  • Existing code dates back almost 15 years
  • Existing system built around pre-new gTLD assumptions
  • Running into technical limits expanding current system so we have an underlying need to rebuild (not related to number of TLDs!)
• Post-transition, along with the re-write, presents us a great opportunity to rethink how key components work
  • AC/TC model dates back decades
  • Technical check process needs improvement
Current RZMS

Root Zone Management

Overview

My domains
This is the list of domains you manage. To review the current details or to make changes to your domains, click the "Domain" link.

<table>
<thead>
<tr>
<th>Domain</th>
<th>My role(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>.ripencc</td>
<td>Technical Contact, Administrative Contact</td>
</tr>
<tr>
<td>.int</td>
<td>Technical Contact, Administrative Contact</td>
</tr>
<tr>
<td>.xn--2zw1k6d</td>
<td>Technical Contact, Administrative Contact</td>
</tr>
<tr>
<td>.xn--11b3b2a2p5g</td>
<td>Technical Contact, Administrative Contact</td>
</tr>
<tr>
<td>.xn--88ahbyktj1f</td>
<td>Technical Contact, Administrative Contact</td>
</tr>
<tr>
<td>.xn--17-rrbytj5a</td>
<td>Technical Contact, Administrative Contact</td>
</tr>
<tr>
<td>.xn--88ahbyktj5a</td>
<td>Technical Contact, Administrative Contact</td>
</tr>
<tr>
<td>.xn--88ahbyktj5a</td>
<td>Technical Contact, Administrative Contact</td>
</tr>
<tr>
<td>.xn--88ahbyktj5a</td>
<td>Technical Contact, Administrative Contact</td>
</tr>
<tr>
<td>.xn--88ahbyktj5a</td>
<td>Technical Contact, Administrative Contact</td>
</tr>
<tr>
<td>.xn--88ahbyktj5a</td>
<td>Technical Contact, Administrative Contact</td>
</tr>
<tr>
<td>.xn--88ahbyktj5a</td>
<td>Technical Contact, Administrative Contact</td>
</tr>
<tr>
<td>.xn--88ahbyktj5a</td>
<td>Technical Contact, Administrative Contact</td>
</tr>
<tr>
<td>.xn--88ahbyktj5a</td>
<td>Technical Contact, Administrative Contact</td>
</tr>
</tbody>
</table>

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

There are no outstanding requests.

Additional Information
This information is published in the Root Zone Database and/or IANA website to assist customers in finding information about the top level domain.

Registration URL: http://www.iana.org/int-domains/nt.htm
WHOIS Server: WHOIS.IANA.ORG
RDAP Servers: —
The pitch — a new authorization model

• Create a new model 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. Performed significant outreach to ccTLD managers but need gTLD feedback too.
• Can accommodate the current arrangement if you like (i.e. two parties who cross-approve all change request types)
• All benefits and no downsides?
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

Authorising Contacts
1. Not published (managed via RZMS)
2. Approves change requests

New Flexible Model

Transition process

- One or more (no fixed number)
- Must be persons (no role accounts)
- Stronger identity controls
- Flexible threshold approval options
- In-country requirements?
Key concepts

Manage authorisers
For each domain you appoint one or more authorizers. These are contacts involved in reviewing changes and providing appropriate approval for those changes.

Authorization model

<table>
<thead>
<tr>
<th>Authorizer Types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joint authorization</td>
<td>All registered authorizers must approve of a change before it can proceed.</td>
</tr>
<tr>
<td>Threshold authorization</td>
<td>Requests will be deemed authorized once the threshold of approvals has been met.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authorizers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naela Sarras</td>
</tr>
<tr>
<td>Kim Davies</td>
</tr>
<tr>
<td>Michelle Cotton</td>
</tr>
</tbody>
</table>

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.)


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

kim.davies@iana.org