Root Zone Management Review and Computing Systems

SUBGROUP MEETING, 12 June 2020

Table of Contents

TOPIC 1: User Instructions *1*

1. **Why this clause is in the contract** **2**
2. **Discussion about how procedures vs. policy is represented in the user guides** **2**
   Draft Statement of IFRT's Findings/Recommendations 3
3. **Frequency and process for reviewing and updating the user guides** **3**

TOPIC 2: Computing Systems *3*

1. **Root Zone Management System (RZMS)** **4**
2. **How PTI Audits reviewing PTI's computing systems** **5**

TOPIC 3 ..... *6*

1. **Authenticate Checks on Customer Requests** **8**
2. **RZM Policy and RFC1591** **9**

TOPIC 1: User Instructions

Article IV, Section 4.6: User Instructions:
Contractor shall, in collaboration with all Interested and Affected Parties, maintain user instructions for the IANA Naming Function, including technical requirements. Contractor shall post such instructions at iana.org ("IANA Website").

Root Zone Management: User Instructions and Guides at
https://www.iana.org/domains/root/help

1. Why this clause is in the contract

NTIA would not allow IANA to publish user instructions, amongst other things, since there was no provision in the contract regarding publishing this. ICANN ensured this made it into the 2013 contract revisions.

Rick: reviewed materials in advance. Feels they are consistent with IANA's processes and meet contract requirement.

2. Discussion about how procedures vs. policy is represented in the user guides

Fred: some policies not reflected in guides; in IFRT report wants to list what is not covered in user documentation. Policy root zone changes, how IANA manages it, needs more coverage.

Kim: https://www.iana.org/help/obtaining-consent
Process is current. Will change the documentation if the process changes due to policy changes.

Peter: IFRT shouldn't be reviewing the detail of the document content itself, but at the topics and structure of offering documentation. Sees difference between Eligible top level domain streams document is not a "process" but "information"; normative vs. informative. Procedures for community involvement in IANA related policies.

Kim: IANA doesn't set policy; just set operations so concern over normative vs. informative documentation may not hold value. Current documentation seems useful for customers on how IANA works. How do we drive documentation? – user demand; operational changes. Is your question really what kind of consultation do we do with customers when we change our operational procedures? There is no change process per se (ie. Decision tree): We discuss internally and determine who needs to be informed, vs. who needs to consent: typically it is RZERC, ICANN Board of Directors; impacts on publication of RZM- involve the RZM which is Verisign and Root Zone Operators. If no external impacts on IANA's partners, then we dicsuss if it's a material impact on customers and we would go to ccNSO, GNSO. Technical Workshop DNS OZARK other options. Contractual change?- then there is specific process. Incremental minor changes may not need any consultation such as requests to add support for addl algorithm types in root zone and we only worked with Verisign on this.

Peter: acknowledges Micromanagement vs processes distinction.

Fred: we are discussing better policy description that could be outside of user instruction, but also referenced within user instructions so that when reading user instructions it tells you what policy each point derived from.

Kim: “policy” – IANA firmlhy doesn’t set policy. We are implementing policy and concerns of starting to quote policy within user instructions. Other groups have very specific definitions of policy…just using this word could cause concerns about IANA getting involved in policy. Does agree we lack well stated policies. IANA derives the “policy” we follow from different sources. Often the policy is vague but IANA still has to figure out how to operationalize them.

Draft Statement of IFRT’s Findings/Recommendations

The current text in things posted on (cite reference material) meets requirements of Article IV, Section 4.6: User Instructions. However the review team notes the content contains mix of instructions & policy and team [may] suggest that IANA works on separating content to provide more pure form of instruction and in next iteration of such content to allows more amateur users clearer instructions for utilizing IANA website.

3. Frequency and process for reviewing and updating the user guides

Fred: frequency of reviewing protocols? Regular cadence might be good process.

Kim: have annual technical discussions with Verisign.

Fred: community participation and what is user instructions to use RZM and what is policy and how it should evolve regarding information that needs to be included in user instructions? Need to define.

TOPIC 2: Computing Systems

Article XI, Sections 11.1 to 11.3 Computing Systems, Notification Systems, Data
Section 11.1 Computing Systems. With respect to the performance of the IANA Naming Function, Contractor shall install and operate all computing and communications systems in accordance with best business and security practices. ICANN and Contractor shall implement a secure system for authenticated communications to Contractor’s customers when carrying out the IANA Naming Function pursuant to the terms of this Contract. ICANN and Contractor shall document practices and configuration of all systems.

Section 11.2 Notification Systems. Contractor shall implement and thereafter operate and maintain a secure notification system at a minimum, capable of notifying TLD registry operators, of such events as outages, planned maintenance, and new developments. In all cases, Contractor shall notify ICANN of any outages.

Section 11.3 Data. Contractor shall ensure the authentication, integrity, and reliability of the service data in performing the IANA Naming Function.

Framework of Interpretation and Delegation of ccTLDs (FOIWG):
https://ccnso.icann.org/en/workinggroups/foiwg.htm

Root Zone Management: User Instructions and Guides at
https://www.iana.org/domains/root/help

1. Root Zone Management System (RZMS)

Kim: Main system is Root Zone Management System: RZMS for tld managers at www.rzm.iana.org, they can submit change requests; interact with pending change requests; etc. also access historical requests.
Back-end is a work flow management system, and guides request through operational phases up to validating that the change was done correctly through automation. Automates automation emails; technical checks; interacts with Verisign who publishes root zone data. Administration interface for PTI staff.

Internal limitation for PTI users for control & security.

Ground up re-write of system is currently going on (system is 17yrs old) and architecture was too limiting. 2 years ago started re-write which is on-going. Will provide basis to then make major changes going forward.

Ticketing System: off-shelf Request Tracker. Open source. Original company makes changes for us to customize. Use across all IANA services. On RZM, used for transactions where a lot of customer communication required like ccTLD delegations and transfers required much due diligence. RZMS not suited for this, but is linkage between RZMS and RT (RT has access to RZMS activities.). IP address of root server would be processed though RT.

Deployment; 2 data centers (west/east coast US) replicas Run active/active and some active/passive. Run active/passive for RZMS so east is secondary/west primary.

Peter: we are not to evaluate system; just check that there is. Some of documentation on system is confidential, so should we note that for next IFR, to determine whether or how this review of systems should go. Contract says it should be documented but not for whose benefit.

Kim: NTIA when contract sections added; annual audit audits our systems in much more explicity detail on how we satisfy various controls. NTIA accepted audit as proof.

2. How PTI Audits reviewing PTI's computing systems

Peter: audit- PTI is obliged to this audit in this contract so is contract double requiring same thing? Review team can assume audit ensures this section has been fulfilled.

Kim: we cannot dictate that to IFRT but we can state that the audit framework has been in place for time-period of review; team's choice to trust audit or not as fulfilling purpose of the IFR. Feel that these 3rd party audits are more thorough than ICANN Community Reviews and we have 2 FTE staff on PTI hwo just runs our audit program (16 people total in PTI). So audits are thorough, comprehensive.

Fred: isn't the audit a security one? The contract language is calling for more than security.

Kim: it's a security audit in the broadest meaning of the word. We audit against 3 of the 5 Trust Services Principles and Criteria. The results are dependent on our operational success.

The Trust Services Principles and Criteria is an international set of principles and criteria developed and managed jointly by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). The SOC 2 and SOC 3 examination is a rigorous process developed by the AICPA and CICA to provide independent assurance that an organization's systems are reliable. Our SOC certification and reports focus on the following Trust Services principles:

- *Availability — the system was available for operation and use, as committed or agreed*
- *Processing Integrity — the system processing was complete, accurate, timely, and authorized*
- *Security — the system was protected against unauthorized access. Each principle is supported by well-defined and detailed criteria that encompass a company's infrastructure, software, data, people, and procedures.*

Peter: audit evaluates systems against ISO standardized criteria. What was behind doing the audit – just this contract, or another obligation?

Kim: History of the audit is we started it in 2010 when we began signing the root zone and we audited against SOC3. Started the SOC2 audit for how we process change requests in 2013. (previously called SysTrust). This framework is similar to ISO, but after working with NTIA we determined the SOC framework was best. Draft PTI strategic plan up for Public Comment and identified need to review audit framework over the next 4 years.

Peter: I don't see any audit gaps.

Rick: SOC2 is harder to pass then the SOC3.

Kim: SOC3 is public attestation about fitness of the system. SOC3 originally pass/fail audit. One "exception" would fail you. Use SOC3 for KSK Operation attestation, so for all 10 years we have done it says "the KSK was operated to 100 % of all controls."

SOC2 is different audience….private assessment, only available to those who have full understanding of system being tested. Detailed assessment with meaningful analysis and so it is confidential. Schematics of network design, details of implementing and deploying systems. This is more useful – not pass/fail, but if you have an exception it provides enough details that you are able to understand how to fix the problem. WE provide this so the people we do business with: Chairs of IETF, IAB, RIRs, ICANN Exectuives.

No provision for independent auditor to provide a public opinion. Auditor gives us a private opinion. IETF reviews it and notifies general management if they are satisfied with it….indirect opinion.

ICANN wanted a system to provide status updates on requests, NTIA said no, so we put it in the contract that we would have a notification system…..this is the background of why we have these clauses in the contract.

We have life-cycle management of all tools (laptops, etc), on-board/off-board staff, staff has limited privilege so they can only access systems/info that pertains to their work. Priveleged access scope limited to staff member's job.

Fred: SOC2 is clean and thorough report. These contract sections are completely covered by SOC2.

TOPIC 3

Annex A, 1 (a) Root Zone Management

a. *The Root Zone Management component of the IANA Naming Function is the administration of certain responsibilities associated with the Internet DNS root zone management.*
b. *Contractor shall collaborate with Interested and Affected Parties to develop, maintain, enhance and post performance standards for Root Zone Management. Specifically, Contractor shall perform Root Zone Management in accordance with the service levels set forth in Section 2.*
c. *Contractor shall also implement DNSSEC in all zones for which ICANN has technical administration authority.*

d. *Contractor shall facilitate and coordinate the root zone of the domain name system, and maintain 24 hour-a-day/7 days-a-week operational coverage. Contractor shall work collaboratively with the Root Zone Maintainer, in the performance of this function.*

   i. *Contractor shall receive and process root zone file change requests for TLDs. These change requests include addition of new or updates to existing TLD name servers ("NS") and delegation signer ("DS") resource record ("RR") information along with associated "glue" (A and AAAA RRs). A change request may also include new TLD entries to the root zone file. Contractor shall process root zone file changes as specified in Section 2 of this Annex A.*

   Contractor shall verify that all requests related to the delegation and redelegation of generic TLDs are consistent with the procedures developed by ICANN.

   Contractor shall maintain an automated root zone management system that, at a minimum, includes (A) a secure (encrypted) system for customer communications; (B) an automated provisioning protocol allowing customers to manage their interactions with the root zone management system; (C) an online database of change requests and subsequent actions whereby each customer can see a record of their historic requests and maintain visibility into the progress of their current requests; (D) a test system, which customers can use to meet the technical requirements for a change request; and (E) an internal interface for secure communications between the Contractor and the Root Zone Maintainer.

ii. Contractor shall maintain, update, and make publicly accessible a Root Zone registration database with current and verified contact information for all TLD registry operators. The Root Zone registration database, at a minimum, shall consist of the following data fields: domain status and contact points for resolving issues relating to the operation of the domain (comprised of at least organizational name, postal address, email address and telephone number). Contractor shall receive and process root zone registration data change requests for TLDs.

iii. Contractor shall apply existing policies in processing requests related to the Delegation, Revocation and Transfer of ccTLDs, including RFC 1591 as interpreted by the FOI and any further clarification of these policies developed by the ccNSO, as appropriate under ICANN's Bylaws, and approved by the ICANN Board. In addition to these policies, Contractor shall, where applicable, consult the GAC 2005 ccTLD Principles. If an existing policy framework does not cover a specific situation, Contractor will use commercially reasonable efforts to consult with and provide opportunity for input from Significantly Interested Parties and, where necessary, may request the ccNSO to undertake policy development work to address such issues.

iv. Contractor shall apply existing policy frameworks in processing requests related to retirement of a ccTLD, including RFC 1591 as interpreted by the FOI and any further clarification of these policies developed by the ccNSO, as appropriate under ICANN's Bylaws, and approved by the ICANN Board. If an existing policy does not cover a specific situation, Contractor will use commercially reasonable efforts to consult with and

provide opportunity for input from Significantly Interested Parties and, where necessary, may request the ccNSO to undertake policy development work to address such issues.

1. Authenticate Checks on Customer Requests

Kim: RZM – maintain content of root zone and meta data around that to authenticate request and review against policy requirements. Public database that we operate using systems mentioned above and there are multiple phases of processing a request. We accept requests from anyone but in business process we ensure the request is clear and well formed and complete. "well form-ness check" is performed.

2nd phase: perform technical checks: check for errors in what was submitted- is it accurately reflecting data; are they referring to servers we can connect to and reach. We're not checking servers against practices, we are just trying to catch common areas we can authenticate. This Test was developed in 2007 and we have used it sense, but it might be over-do for review and revisions- PTI staff have some ideas. Other guiding philosophy for technical check is safeguard that this authorized by tld operator. If you want to make change to a name server set (NS records)or ds record, dns, do bit set record that change should have already been effected in zones you control. Ns record update request, then it should have been updated in tld zone first. If you are requesting a ds change, you should have made a match dns key in the tld zone. Typo checks. If party had capability of editing the tld zone then they pass one test towards. Hostile attackers would already have taken over critical system of tld control, so us changing the root zone isn't making a big difference to the attack.

Authorization: anyone can submit request, but has to be authorized. Administrative and technical contact on file for tld need to co-authorize change request. In event if name server change shared by multiple tlds we'll ask for authorization from other tlds as well.

Staff processes request live and do own checks: check any sanctions or regulations pertaining to tlds are satisified and we comply with laws. If it is a material transfer of tld from party to another, we check rules around that. Gtld needs contractual amendment with ICANN, cctld we do due diligence and perform analysis that request is OK to move forward. Public report is drafted and sent to icann board and will make decision about proceeding.

Implementation for non-root zone changes happens immediately. NS, Ds, Blue record sent to Verisign via EPP, they re-perform some same technical checks and some checks that check PTI did it correctly. Implement change in 24hrs and then it gets published. PTI check that root zone files did change.

Verisign through polling over EPP protocol. Ns set for root servers done over epp – recently development 1 or 2 years ago. Customized version of epp.

DNS SEC as configured at high level KSK vs ZSK. PTI operates KKS. Verisign operates ZSK – short lived keys generated – 90 days of ZSK for PTI to sign with KSK ceremony, KSK is trust anchor for DNS, we recognize the unique considerations of risk of disclosure, if tld loses key then they can roll their key and make an emergency change. But PTI doesn't have that luxury like a tld does, so we need extra precautions.

Relationship of IANA and Root Zone Maintainer. PTI needs to work with RZM and we are not allowed to do same work as RZM. RZM needs to be audited too like PTI is? No. RZM contract is different than this contract. No audit requirement in RZM contract.

2. RZM Policy and RFC1591

RFC1591 – 1994 published. Intended to be a user guide. Now interpreted as policy. FOI is ccNSO's S Framework of Interpretation and Delegation of ccTLDs (FOIWG): https://ccnso.icann.org/en/workinggroups/foiwg.htm which provides implementation guidance on interpreting RFC1591.

Obligation for PTI to do consultation if policy is insufficient in covering situations. PTI did that – like identifying lack of guidance for retiring tlds. Pushing ccNSO to take this on and hope it's near completion.

Peter: draft retirement policy still in public comment period, contract shall apply existing policies ccNSO will not go through all requests in recent years. Re-delegation requests documented on IANA website. ccNSO usually reviews ever incidence of prior happening, and working group may review all instances of cctld transfer and analyze it.