Verisign/ICANN Proposal in Response to NTIA Request

Root Zone Administrator Proposal Related to the IANA Functions Stewardship Transition

Introduction

On March 14, 2014, NTIA announced its intent to transition key Internet domain name functions to the global multistakeholder community. As the first step, NTIA asked the Internet Corporation for Assigned Names and Numbers (ICANN) to convene global stakeholders to develop a proposal related to the stewardship of the Internet Assigned Numbers Authority (IANA) function. Just over 17 months later, stakeholders have issued a draft proposal on this as well as a proposal to enhance the accountability of ICANN, with the intention of a final package coming to NTIA later this year.

In order to prepare for the implementation phase of the IANA stewardship transition, NTIA has asked Verisign and ICANN to submit a proposal as to how best remove the NTIA's administrative role associated with root zone management in a manner that maintains the security, stability and resiliency of the Internet's domain name system. This proposal offers a high-level plan for the transitioning of the NTIA role for consideration along with joint recommendations from Verisign and ICANN on the way forward.

Background

The Root Zone Management System (RZMS) is a set of tools, which currently allows ICANN as the IANA Functions Operator (IFO), Verisign, as the Root Zone Maintainer (RZM), and the National Telecommunications and Information Administration (NTIA) at the U.S. Department of Commerce (DoC), as the Root Zone Administrator (RZA), to collaboratively manage the changes to the Internet's single authoritative root zone. The current automated RZMS replaced the legacy root zone update, validation, extraction, and distribution methods with a web based user interface (UI) that permits Top-Level Domain (TLD) managers to submit change requests, an Extensible Provisioning Protocol (EPP) client and server system that communicates incoming root zone change requests between the IFO and the RZM, two web-based authorization UI portals for NTIA use, a set of special RZMS web based UIs for ICANN and Verisign to facilitate administrative management of change requests, customer service representative (CSR) tools to allow IFO and RZM staff to perform functions such as checking domain history and accommodating any required manual updates, and dedicated mail servers for sending and receiving encrypted and signed RZMS-related electronic messages.

There are three key components of the DNS that are managed by the RZM in conjunction with the IFO and are required for proper function of the DNS root. Those key components are 1) the root zone, 2) the root-servers.net zone, and 3) the root hints file. All three of these work products are produced utilizing the same process and procedures and currently require NTIA authorization for changes. In addition, there are supplemental items that require NTIA authorization related to DNSSEC specifically, the Signed Key Response (SKR).

The functions and capabilities of the root zone have been modified from time to time via the NTIA's and U.S. Government's procurement processes through specific requirements identified through the issuance of Requests for Proposals for the NTIA to acquire services to manage the three components and others identified above. Specific requirements for these modifications can be generated from a number of sources but most prominently have been identified through a Notice of Inquiry (NoI) process seeking public input on required functions as well as developed standards to improve services that come from the likes of the National Institute of Standards and Technology (NIST) or the Internet Engineering Task Force (IETF). This aspect of NTIA's role in root zone management is not addressed within this Proposal as it is assumed to be covered via the ICANN community's transition proposal(s).

Figure 1 illustrates the relationship between the three parties involved in root zone management and their respective functions and roles.

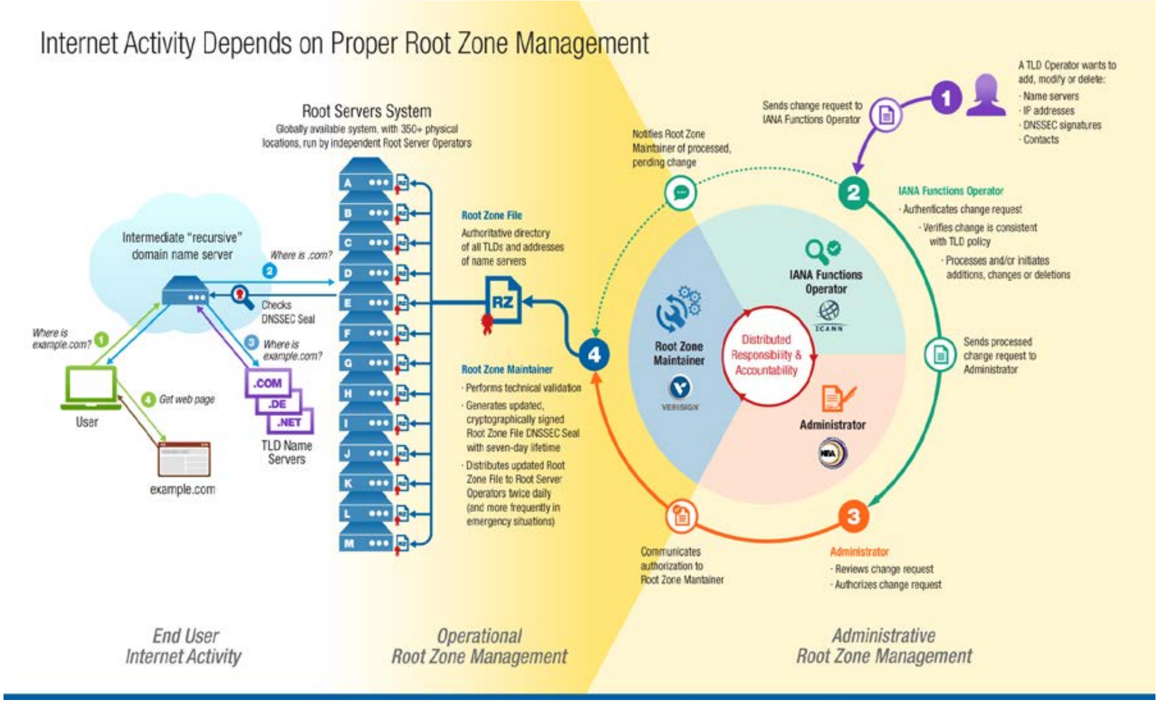
Internet Activity Depends on Proper Root Zone Management
Root Servers System
Globally available system, with 350+ physical locations, run by independent Root Server Operators
A
B
C
D
E
F
G
H
I
J
K
L
M
Intermediate "recursive" domain name server
Where is .com?
2
Checks DNSSEC Seal
Where is example.com?
1
3
Where is example.com?
User
4
Get web page
example.com
.COM
.DE
.NET
TLD Name Servers
Root Zone File
Authoritative directory of all TLDs and addresses of name servers
RZ
Root Zone Maintainer
· Performs technical validation
· Generates updated, cryptographically signed Root Zone File DNSSEC Seal with seven-day lifetime
· Distributes updated Root Zone File to Root Server Operators twice daily (and more frequently in emergency situations)
4
A TLD Operator wants to add, modify or delete:
· Name servers
· IP addresses
· DNSSEC signatures
· Contacts
1
Sends change request to IANA Functions Operator
Notifies Root Zone Maintainer of processed, pending change
2
IANA Functions Operator
· Authenticates change request
· Verifies change is consistent with TLD policy
· Processes and/or initiates additions, changes or deletions
IANA Functions Operator
ICANN
Root Zone Maintainer
VERISIGN
Distributed Responsibility & Accountability
Administrator
NTIA
Sends processed change request to Administrator
3
Administrator
· Reviews change request
· Authorizes change request
Communicates authorization to Root Zone Mantainer
End User Internet Activity
Operational Root Zone Management
Administrative Root Zone Management

Figure 1: The Root Zone Management Functions

IANA Functions Stewardship Transition

According to the current transition proposal by the IANA Stewardship Transition Coordination Group, the RZA role currently performed by NTIA will be eliminated upon the completion of the transition.

Root Zone **Administrator Proposal**

ICANN and Verisign propose an approach to the RZA role removal in which the full root zone management system as it functions today is replicated in another instance with a new unique set of credentials for authentication (versus “authorization”) of Root Zone Change Requests (“RZCRs”) or SKRs. In this approach, no code changes are required and only one single authorization action remains possible. The two systems would operate in parallel, with the IFO replicating TLD manager change requests entered into one instance into the second instance, and the RZM verifying the results generated by the two instances are identical just prior to the newly updated and signed root zone on the RZM distribution master server.

To implement this approach, the existing components of the IFO, RZA, and RZM systems will be duplicated and new client certificate information with new user credentials to the two root zone change administrator portals, as well as the SKR Authorization/Authentication portal will be created. We call these new credentials “RZA2” where the A stands for authentication. The duplicate authentication portal that accepts the RZA2 credentials would be accessed from a new specific location and the same authorization/authentication response as the RZA would be entered for a determined period of time (the “parallel operation” period) to ensure that the resulting zone file was produced in exactly the same form.

During the testing phase in this scenario, ***both*** RZA and RZA2 will authenticate to their respective root zone change portals and authorize RZCRs and SKRs. This approach requires no code changes to the portals, but would involve at least the following tasks:

- Provisioning and deployment of identical sets of respective RZMS systems for the IFO and RZM.
- Access Control List (ACL) updates on network equipment
- Database updates to add new users and client certificates
- Development of software or processes to duplicate RZCRs entered by TLD managers into the IFO web user interface and submission of those duplicate RZCRs into the RZA2 instance
- Development of software or processes to duplicate SKRs provided by the RZM to the IFO and KSRs provided by the IFO to the RZM
- The ability to generate (but not publish) a parallel DNSSEC-signed zone
- Development of software that compares and certifies the published zones identical
- Twice daily comparisons of zones
- Publishing of comparison results
- Certification that the parallel operation time frame has been achieved with zero deviations in results or with clearly defined and acceptable external causes with proposed mitigations
- Define and test a process to resolve any discrepancies found during the twice-daily comparison of the zone files

With respect to the parallel operation time frame, it would be prudent to use the same approach as that taken during the efforts to DNSSEC sign the root zone. Specifically, the output of the actions taken by the IFO, RZA2, and RZM should be monitored for a mutually agreed period of time. If no deviations are detected and determined to be caused by differences between RZA and RZA2 within that time period, success is declared. However, if unexplained deviations are detected, the clock measuring the time period is reset to zero, thereby requiring another full time period without unexplained deviations to be observed.

In order to minimize changes to the code base during the implementation, ICANN and Verisign are proposing to have the IFO perform an authentication action to take the place of the authorization currently performed by NTIA in the parallel system. From an external perspective, since the authorization/authentication would be done immediately after the transmission of a root zone change request, there would be no perceptible delay in processing of those requests. Since the changes to the RZMS code to remove the authentication action require coordination between ICANN and Verisign and those changes will require extensive testing in the Operational Test & Evaluation (OT&E) environments of both organizations, the current plan is for ICANN and Verisign to revise the RZMS code to remove the authorization "call out" after the transition in order to not impact the transition timeline.

In the event of technical issues being encountered during the processing of root zone change requests, in the typical case, that is, when a technical issue is discovered during the IANA technical checks, those technical issues would be dealt with as they are handled today with ICANN staff working with the TLD managers to address the issues prior to progressing the change request to Verisign. In the event that Verisign detects a technical issue after the IANA technical checks, an exception would be raised, and Verisign and ICANN would address the issues, similar to the how these issues are dealt with today.

It should be noted that until the transition is complete, the authoritative root zone file would be the one that has authorization performed by NTIA and not the one authenticated by RZA2. While the root zone generated by the parallel system will be identical to the authoritative root zone, it will not be placed upon the distribution master. If there is any discrepancy between the authoritative root zone file and the zone file generated by the parallel system, an exception would be raised and the cause of that discrepancy would be identified and addressed.

With respect to manual changes, such as the removal of TLDs and/or changes to the root-servers.net zone, such changes will be handled in the parallel system the same way they are handled today except without the involvement of NTIA. Specifically, the changes (once requested by the appropriate/verified party) will be vetted by the IFO and coordinated via direct communication with the RZM that will implement the changes after consensus is reached.

During the parallel testing period, ICANN and Verisign will provide monthly reports documenting activities performed during testing, any exceptions raised and how they were addressed, and other information deemed of interest to NTIA. The format of these monthly reports will be mutually agreed between NTIA, ICANN, and Verisign. In addition, ICANN and Verisign will provide a joint final written report documenting the outcome of the testing of the RZA transition mechanisms described in this proposal and that final report will include the implementation plan that will be used to implement the

RZA transition.

It should be noted that nothing in this proposal is intended to preclude alternative RZA transition mechanisms being jointly proposed by ICANN, Verisign, and/or NTIA. In the event an alternative RZA mechanism is identified in advance of the IANA stewardship transition, it can replace the mechanism proposed in this document by mutual agreement of all parties.

Recommendations

We recommend that the fewest new credentials as possible for the RZA2 be added to the system and that NTIA and the RZA2 agree on how to compare resultant zone files. It is our recommendation that the cleanest and most secure way forward would be to make the appropriate code changes to the system that would require both parties, NTIA and RZA2, to authorize/authenticate each change during the parallel operation period with the RZM to publish daily reports on the comparison results. These reports will be publically posted to ensure transparency and community monitoring.

ICANN and Verisign propose a 3-month successful parallel operation period. That is, after the parallel operation period is initiated, success will be declared if there are no unexplained deviations from expected results caused by differences between RZA and RZA2 after 3 months. If a deviation is found without appropriately documented external conditions or the NTIA in its role determines that modifications are required to the RZMS, the 3-month clock will be reset to zero, requiring another 3 months with no deviations before success can be declared.

Following these recommendations would limit any confusion from the shared responsibility of the authorization/authentication role and be a transparent separation of duties, while also educating the RZA2 on actions and consideration given by NTIA in its current RZA role. Then following the “parallel operation” period where both the RZA and RZA2 are authorizing and authenticating respectively all RZCRs, the RZM will make a configuration change to the RZMS system thereby eliminating the need for both RZA’s authorization/authentication, leaving just the RZA2 to provide all future RZCR and SKR authentications.

NTIA Q and A on the
Root Zone Administrator Proposal Related to the IANA Functions Stewardship Transition

Q. What does this proposal do?

A. The proposal establishes an approach to develop and test a mechanism to manage the root zone in the absence of NTIA's Root Zone Administrator authorization role, in a manner that maintains the security, stability and resiliency of the root before and after the IANA stewardship transition.

Q. Does this proposal impact the multistakeholder community's IANA Stewardship Transition process and/or proposals?

A. The proposal was prepared in response to a March 4, 2015 request from the NTIA. The proposal should complement the multistakeholder community's IANA Stewardship transition process and proposals regarding the RZA (NTIA) role.

Q. When did Verisign and ICANN begin work on this proposal?

A. The proposal was prepared in response to a March 4, 2015 letter from NTIA to Verisign and ICANN. The letter requested that they work together to develop the proposal. The discussions and the development of the proposal have been conducted in confidence at Verisign's request, for commercial business reasons, until the work on the proposal was complete.

Q. Will anything change immediately between NTIA and Verisign as a result of this proposal?

A. No. Until the IANA stewardship transition is completed, Verisign, at the direction of NTIA, plans to continue its current role as Root Zone Maintainer (RZM) under the Cooperative Agreement with the Department of Commerce.

Q. Will there be a new agreement to perform the RZM function post the IANA stewardship transition?

A. Verisign performs the RZM function today, including multiple daily publications of the root zone file, under the Cooperative Agreement with the Department of Commerce. It is anticipated that performance of the RZM function would be conducted by Verisign under a new RZM agreement with ICANN once the RZM function obligations under the Cooperative Agreement are completed.

Q. Has a final new RZM agreement between Verisign and ICANN been completed?

A. No.

Q. Does this proposal or the anticipated new RZA agreement impact Verisign's .com or .net registry agreements?

A. No. This proposal and the IANA stewardship transition do not impact the .com and .net registry agreements. RZM is a separate function performed at no cost as a public service by Verisign spanning three decades.

Q. How will this impact the Cooperative Agreement between NTIA and Verisign?

A. The Cooperative Agreement between NTIA and Verisign will continue. Once the parallel testing for root zone management has proven capable of performance in the absence of the RZA / NTIA role and the IANA Stewardship transition implemented, NTIA and Verisign will amend the Cooperative Agreement as appropriate.

Q: Will there be any change to any production root zone management policy or process?

A: No. The only change will be the creation of a parallel process in which the role performed by NTIA in authorizing root zone changes will be replaced by ICANN authenticating the same changes. The production RZMS will remain unchanged.

Q: To whom should a TLD operator send complaints in the event of issues during or after the transition?

A: From the perspective of TLD managers and other service requesters, nothing will be changing. Concerns should continue to be sent by email to iana@iana.org or to root-mgmt@iana.org.

Q: Is there any risk that a change implemented and authorized by NTIA will not be implemented by Verisign and instead, a change authenticated by ICANN will be?

A: No. Verisign will continue to publish only the changes authorized by NTIA until the stewardship transition has been completed. However, it should be noted that in normal operation, there would be no difference between the production and the Operational Test & Evaluation (OT&E) systems.

Q: How will the community know that no discrepancies were discovered between the production system and the OT&E system?

A: During the parallel testing period, ICANN and Verisign will provide monthly reports documenting activities performed during testing, any exceptions raised and how they were addressed. These reports will be submitted to NTIA and will be published on the ICANN website for full transparency.