CONTROL IS DEAD, LONG LIVE CONTROL

OLEG DEMIDOV,
CONSULTANT AT PIR CENTER.
IN 2012-2014 OLEG RAN THE PIR CENTER'S PROGRAM "GLOBAL INTERNET GOVERNANCE AND INTERNATIONAL INFORMATION SECURITY".

A KEY COMPONENT OF THE IANA FUNCTIONS in terms of maintaining the security, stability, and resilience of the system of unique Internet identifiers is the business process of managing the DNS root zone. For that reason, its reform (as part of the process of IANA functions stewardship transition) is attracting special attention in the Russian technical community and elsewhere. The key actors in this process are as follows:

- Operator of the IANA (Internet Assigned Numbers Authority) function; this role is currently being fulfilled by the ICANN Corporation. The operator receives, reviews, and processes submissions for entering changes in the DNS root zone file; performs technical validation of the submissions; notifies the operators of the fulfillment of their submissions, and enters changes in the WHOIS root database.
- Administrator of the root zone; this role is currently (until the completion of the IANA functions stewardship transition) being fulfilled by the U.S. National Telecommunication and Information Administration (NTIA). The administrator oversees the processes, procedures and policies that are followed by the operator of the IANA functions; authorizes the root zone maintainer to enter changes in the root zone file upon request from Top Level Domain operators; and authorizes the operator of the IANA function to enter changes in the WHOIS database.
- The maintainer of the root zone; this role is currently being fulfilled by Verisign Corporation. The root zone maintainer enters changes into the root zone file, generates an updated version of the file, and uploads the file to the 13 authoritative root zone DNS servers.

Therefore, while the procedural and bureaucratic part of the process is the responsibility of ICANN and the NTIA, the actual technical work is being done by the maintainer, which is Verisign.

Verisign functions in terms of the business process of DNS root zone maintenance were specified in Cooperative Agreement NCR 92-18742[1] between Verisign and the U.S. government (represented by the NTIA). It was signed on January 1, 1993 by the National Scientific Fund (NSF, whose remit under the contract was later taken over by the NTIA) and Network Solutions, Inc. (NSI, acquired in 2000 by Verisign, which thereby became a party to the Agreement). This is how the business process of DNS root zone maintenance – including operations that are Verisign's responsibility – came into being in 1993-2001. During that period, the DNS root zone file was generated on Root Server A, operated then and now by Verisign.

The original version of the article in Russian is published in the thematic issue of e-journal Cyber Pulse № 3 (21) September 2016

The description of the technical parameters of Verisign functions in this commentary is based on the report "Stability, security, and resilience of the global Internet infrastructure: technical and legal aspects", produced in 2015-2016 by a group of Russian and U.S. experts. The group delivered one of the few currently available Russian—language studies into the organizational, technical, and legal aspects of the history, standardization, functioning, and development of the global system of unique Internet identifiers. The intended audience of the report is the Russian and international technical and Internet industry community, as well as the researchers and experts whose area of professional interest includes the aforementioned aspects of the operation and regulation of the system of unique Internet identifiers. The text of the report in the Russian language is available on the PIR Center website and on the website of the Internet Support Foundation; it is distributed under the Creative Commons Attribution-Non-Commercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) license.

In 2001 the business process underwent significant changes. The DNS root zone master server function was transferred from Root Server A to a new hidden distribution master server, also known as the "hidden master". This server is authoritative for the DNS root zone, and there is no Name Server Record for it. The DNS master servers are usually hidden, so this is by no means unique. Be that as it may, in November 2001, the 13 root servers, including the former Master Server A, became secondary authoritative servers. The new master generates the DNS root zone file, which is then uploaded to the 13 root servers. The upload is done every 12 hours, regardless of whether there have been any submissions (received or processed) for changes in the contents of the file in the intervening period.

The fact that Verisign is a commercial company affects the transparency of the business process of DNS root zone maintenance. In terms of fulfilling these functions, Verisign is accountable only to the U.S. government. Details about the work of the master server operated by Verisign are mostly unavailable to interested parties. Maintaining the hidden master should fall under the scope of the amended Cooperative Agreement between Verisign and the NTIA. But the text of the Agreement does not contain any direct mentions of the hidden master; nor does it explain the need for installing such a server instead of the former primary Server A. Further, Verisign's functions as the DNS root zone maintainer are not included on the agenda of the Root Server System Advisory Committee (RSSAC) under ICANN. Establishment of formal relations between ICANN and the root server operators began with the signing in December 2007 of the Mutual Responsibilities Agreement between ICANN and the Internet Systems Consortium[2]. Another RSSAC document, called "Service Expectations of Root Servers", was published as part of that relationship on December 4, 2015[3]. Verisign's only role in that relationship is to operate Root Server A.

As a result, the global Internet community does not have any open information or a clear idea about the business process of root zone maintenance – unlike, for example, the no less important business process of updating the key signing key (KSK) as part of DNS Security Extensions (DNSSEC) process in the DNS root zone. For the latter process, we have very detailed descriptions of the administrative and technical processes, which give us the full picture of the security and resilience procedures, as well as protocols of the KSK update ceremonies[4].

In that context, the insufficient transparency of the root zone maintenance technical procedures and business processes at Verisign is often criticized by the technical community and other stakeholders. In recent years, these criticisms have increasingly focused on the fact that the status of the root zone maintainer functions remained unclear in the context of the IANA functions stewardship transition. Most of the questions about the Verisign business process, however, remain technical rather than organizational or legal, such as:

- What is the software and hardware used to generate the DNS root zone file?
- How does Verisign ensure the security of the root zone file when it uploads it from the hidden master to the secondary authoritative servers?
- Has there been any standardization in ensuring the security, stability and resilience of the hidden master function and the root zone file upload? Which parts of the technical community were involved in that standardization?
- Is the work of the hidden master subject to independent external audit, and if so, who is the auditor?

Outside parties know only parts of the answers to these questions. It is known, for example, that Verisign uses the Transaction SIGnature (TSIG) protocol to secure the upload of the root zone file. TSIG is a network-level protocol that is mostly used in the DNS, and standardized in RFC 2845[5]. In this protocol, shared secret keys and one-directional hashing are used for cryptographically protected authentication of each connection endpoint. In the DNS root server system, a secret TSIG key is generated thrice a year during informal meetings between root server representatives that take place on the sidelines of the Internet Engineering Task Force (IETF)[6].

It is hard to give a substantive answer to many of the questions without being able to observe the business process itself, or without access to its detailed description. For example, is the use of TSIG enough to eliminate the risk of the root zone file being tampered with during the upload from the hidden master? Is the hidden master itself sufficiently secure, and does it have sufficient redundancy to withstand a major security incident, including a targeted external attack (such as an attempt to replace a root zone file with a doctored version during the upload to the operators of the root zone servers)? Technically, it is clear that the Verisign functions should be more transparent, at least to the technical community.

The debate about managing the unique identifiers system in connection with the IANA functions stewardship transition has drawn additional attention to the status of Verisign. In an NTIA statement of March 14, 2014, which was the starting point for the transfer of the U.S. government's coordinating role, the role of the DNS root zone maintainer in the current architecture of managing the unique identifiers was mentioned among other issues that should be resolved as part of the so-called IANA Transition process. The neutral phrasing of the statement did little to hide the obvious message: if the NTIA is withdrawing from the system of relations connected to the IANA functions, then clearly the U.S. Department of Trade should also withdraw from its direct contractual relationship with Verisign. Otherwise, the entire process would be little more than a half-measure because the U.S. government would retain its de facto control of the technical processes in the DNS root zone.

Even more radical ideas have been voiced on the sidelines of various international meetings and discussions. Verisign does not have any exclusive right to fulfil the function of the root zone maintainer, though it does have a wealth of experience in the matter and a well-established business process. Nevertheless, the process itself is not uniquely challenging or resource-intensive; it does not require the development and maintenance of any complex infrastructure. It is in fact quite simple, and requires only a single site (provided that there is adequate redundancy) to run smoothly. It does not have a complex hierarchy of processes; it has very few participants, and it has a bare minimum of the external perimeter that could potentially be used for an external attack. It is, however, critically important for all Internet users, governments, and businesses because it directly underpins the work of the global DNS (though not the work of the Internet as such) – hence the insistent questions being asked about it. In other words, there are many other entities that could do the job equally well.

Representatives of the Russian Internet community have voiced the following two ideas: 1) Verisign functions should be transferred to IANA itself (or rather, to the PTI), thereby removing the unnecessary third party, and 2) Verisign functions should be transferred to a neutral technical entity that is independent from ICANN (unlike the PTI, which is after all an affiliate of the Internet Corporation). Implementing these ideas would be a major step towards the separation of the IANA functions, which has become one of the key principles in the stewardship transition. Possible candidates for the role of the root zone maintainer include RIPE NCC, one of the most active and advanced regional registries. For both of the aforementioned Russian proposals, however, there is an unfortunate reservation: the United States and Verisign itself would never allow them to be implemented. Verisign would be led by purely commercial considerations; being the root zone maintainer is a major symbolic and reputational asset. The U.S. government, for its part, would not allow Verisign functions to be transferred to a foreign entity because it wants any future DNS root zone maintainer to remain in U.S. jurisdiction. It has no interest in launching a garage sale of its supervisory powers, and the Republicans in Congress would surely go berserk at such a turn of events.

After the launch of the IANA functions stewardship transition process in 2014, the root zone maintainer issue somehow fell off the back of the wagon, and up until the second half of 2015, attempts to restart this public discussion at ICANN conferences went for naught. The question was, however, discussed privately between ICANN, the NTIA, and Verisign itself. The decisive factor was probably the pressure put on ICANN by the ICG, which consistently – and fairly – argued that without the NTIA's withdrawal from the root zone maintenance arrangement, the entire transition process would be pointless. By October 2015, the decision to exclude the NTIA from root zone maintenance and to draw up a new cooperative agreement between ICANN and Verisign had been taken and formulated in an ICANN/Verisign Joint Proposal on root zone administrator functions[7].

The decision was reflected in March 2016 in the final Proposal submitted for the NTIA's consideration by the Coordinating Group for the IANA Functions Stewardship Transition[8]. The Proposal noted that after the completion of the transition, the anticipated agreement between the PTI and the root zone maintainer would be required once the NTIA has withdrawn from the DNS root zone maintenance process. The Proposal also emphasized that the complete and final transition of stewardship would require a revision of the relationship between the current IANA functions operator (ICANN), the current DNS root zone maintainer (Verisign), and the current root zone administrator (the NTIA). The key point here is that the Proposal, which was quickly accepted by the NTIA, stated that before the completion of the IANA functions stewardship transition, ICANN and Verisign should sign a written agreement without the NTIA, and that the agreement should be made available for public review before it enters into force[9].

The draft agreement on DNS Root Zone Maintainer services between the Internet Corporation and Verisign was released for public review on June 29, 2016. In August, the draft Agreement was approved by the ICANN Board. The document specifies the following list of Verisign functions, which is somewhat different from the previous list in terms of its phrasing[10]:

- Perform technical validation of the data received from ICANN as part of the DNS root zone change submission;
- Notify ICANN of whether the submission meets the necessary requirements;
- Edit, generate, sign (using DNSSEC), and publish the new root zone file;
- Notify DNS root server operators of the availability of the new file;
- Serve as the Zone Signing Key (ZSK) operator for the DNS root zone;
- Perform emergency root zone file generation at ICANN request.

Verisign is expected to perform these functions for eight years, for a symbolic remuneration of 300,000 dollars a year, paid by ICANN. Importantly, there is now a clearly defined algorithm for appointing a new root zone maintainer.

Another aspect of the draft Agreement, which is especially interesting in the context of the discussion on whether the U.S. government is genuinely relinquishing control of the unique identifiers system, is contained in Article 8, Paragraph d) of the Agreement (Suspension of Services). Under the terms of that article, Verisign may suspend any of the Services and/or Additional Services, in whole or in part, and/or suspend access to its Root Zone Maintenance System (RZMS, which includes the root zone file upload server and an FTP file server) to comply with applicable U.S. laws. Verisign's right to suspend includes, in each case, only to the extent necessary to comply with such Law:

1. revoking the right of access (License) to Verisign RZMS (ICANN needs that access to supply Service Data in order to authorize its root zone change submissions); suspending or otherwise restricting ICANN's access to the Verisign RZMS;
2. stopping the acceptance of Service Data from ICANN;
3. delaying, denying, deleting, freezing, or transferring the Root Zone File, and
4. taking such other action, all as required to comply with such Law.

This section of the draft Agreement makes it perfectly clear that the NTIA's withdrawal from root zone maintenance will in no way deprive the U.S. government of the legal instruments to re-exert full control of the process, if need be. DNS root maintenance still resides in U.S. jurisdiction.

There is a proviso that Verisign shall notify ICANN in advance of any actions to suspend and/or restrict the provision of root zone maintenance services – unless of course such notification would break the law – and that it shall in any case immediately notify the Internet Corporation after taking such action. That is a small consolation, but better than nothing.

The Agreement is still at the draft stage, and it is not clear when it might be signed and enter into force. This is unlikely to happen simultaneously with the expiration of the IANA functions stewardship agreement between ICANN and the NTIA. There is no real need for such synchronicity; it would be sufficient for the community to know that the process is ongoing, and will be completed within a reasonable time frame. In theory, the text of the Agreement might yet change, but the discussion is all but closed. Besides, July 5, 2016 marked the successful completion of a 90-day parallel testing of the new DNS management system directly between ICANN and Verisign[11]. This means that the process is at the final stages, and the global technical community will soon have to live with the new arrangement and with the terms stipulated in the approved draft of the Agreement. Consequently, the debate about the role of the U.S. government in DNS root zone management will continue. The change is not revolutionary, and the DNS root management process fully remains in U.S. jurisdiction.

Does that mean that all attempts at transforming that process over the past two years have failed? Not at all. First, the new configuration of the participants in the process and of the parties to the contract makes it possible to address the technical issues described in this article. Transparency and accountability are the key priorities for ICANN in the long-term process of reforming the governance structure of the Internet Corporation. There is a chance that applying those two principles to the work of the root zone maintainer will make its functions more transparent to the community, and help to build confidence in these functions among the community, including foreign (i.e. non-U.S.) stakeholders. Second, a journey of a thousand miles begins with a single step. It is entirely possible that once the proposed Agreement expires in eight years' time, it will not be automatically extended, and the DNS root zone maintainer functions will be transferred to entities residing in non-U.S. jurisdictions. Or maybe nothing of the kind will happen because everyone will be satisfied with the existing arrangement, and no-one will have any problem with Verisign.

REFERENCES

[1] *Verisign Cooperative Agreement and all the amendments, NTIA http://www.ntia.doc.gov/page/VeriSign-cooperative-agreement (Last accessed September 1, 2016).*

[2] *Mutual Responsibilities Agreement (ICANN and ISC), ICANN http://archive.icann.org/en/froot/ICANN-ISC-MRA-26dec07.pdf (Last accessed March 1, 2016).*

[3] *RSSAC001 Version 1. Service Expectations of Root Servers. An Advisory from the ICANN Root Server System Advisory Committee (RSSAC), 4 December 2015, ICANN https://www.icann.org/en/system/files/files/rssac-001-root-service-expectations-04dec15-en.pdf (Last accessed September 1, 2016).*

[4] *Root Zone DNSSEC KSK Ceremonies Guide. Root DNSSEC Design Team J. Schlyter, F. Ljunggren, Kirei R. Lamb, ICANN, May 7, 2010 http://www.root-dnssec.org/wp-content/uploads/2010/05/draft-icann-dnssec-ceremonies-01.txt (Last accessed September 1, 2016).*

[5] *Root KSK Ceremonies, IANA https://www.iana.org/dnssec/ceremonies (Last accessed September 1, 2016).*

[6] *Secret Key Transaction Authentication for DNS (TSIG), IETF, May 2000 http://tools.ietf.org/html/rfc2845 (Last accessed September 1, 2016).*

[7] *Andrei Robachevsky. The Internet from the Inside Out. Ecosystem of the Global Network. Moscow: MSK-IX, 2015. – PP. 108-109.*

[8] *Verisign/ICANN Proposal in Response to NTIA Request Root Zone Administrator Proposal Related to the IANA Functions Stewardship Transition, NTIA https://www.ntia.doc.gov/files/ntia/publications/root_zone_administrator_proposal-relatedtoiana_functionsste-final.pdf (Last accessed September 1, 2016).*

[9] *Proposal to Transition the Stewardship of the Internet Assigned Numbers Authority (IANA) Functions from the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) to the Global Multistakeholder Community. IANA Stewardship Transition Coordination Group (ICG), March 2016, P. 6, &X017 https://www.icann.org/en/system/files/files/iana-stewardship-transition-proposal-10mar16-en.pdf (Last accessed September 1, 2016).*

[10] *Ibid, p. 7-8.*

[11] *Root Zone Maintainer Service Agreement, ICANN, June 29, 2016 https://www.icann.org/iana_imp_docs/63-root-zone-maintainer-agreement-v-1-0 (Last accessed September 1, 2016).*