ICANN Registry Request Service

Ticket ID: L8G7K-3E9T2
Registry Name: VeriSign, Inc,
gTLD: .COM, .NET, .NAME
Status: ICANN Review
Status Date: 2012-03-20 16:28:12
Print Date: 2012-03-20 16:28:20

Proposed Service

Name of Proposed Service:

DNSSEC Implementation for .name

Technical description of Proposed Service:

Consultation

Please describe with specificity your consultations with the community, experts and or others. What were the quantity, nature and content of the consultations?:

Verisign technical and research staff have been regularly engaged with the technical community on the full spectrum of DNSSEC issues and have worked with organizations and individuals considered to be experts in the field of DNS. The Verisign labs program has been engaged in the DNSSEC technical forums for nearly a decade. Verisign's research and development staff has been a significant contributor to the standards process, working collaboratively with other registries to shape the DNSSEC standards for the NSEC3 protocol addition. NSEC3 has been adopted by several registries that have signed their zones Verisign has contributed to technical discussions and communication of DNSSEC to the Internet community in the following forums:

o DNSSEC Coalition;
o DNSSEC Deployment Working Group;
o DNS-OARC (Operations, Analysis, and Research Center);
o IETF for protocol design and operations related to DNSSEC, which includes extensive participation in working groups to author and finalize the latest DNSSEC RFC's:
o RFC #4033 - DNS Security Introduction and Requirements; Matt Larson (Verisign), et al., March 2005
o RFC #4034 - Resource Records for the DNS Security Extensions; Matt Larson (Verisign), et al., March 2005
o RFC #4035 - DNSSEC Protocol Modifications; Matt Larson (Verisign), et al., March 2005
o RFC #5155 - DNS Security (DNSSEC) Hashed Authenticated Denial of Existence; David Blacka (Verisign), et al., March 2008
o RFC #5910 - Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP); J. Gould et al. (Verisign); May 2010

Since 2008, Verisign has been engaged with the registrar community on the topic of DNSSEC. Verisign has learned that DNSSEC knowledge and experience vary widely among registrars. Verisign conducted surveys in 2009 and 2010 that *included topics on DNSSEC. During the course of 2011, Verisign has seen an increase in the amount of registrars adopting DNSSEC. As of December 2011, more than 40 Registrars have at least one signed domain in the .net or .com domain name space. Statistics from the registrars that responded to the 2010 survey indicate that 75% of the registrars planned to implement within 2 years. The survey also indicates that approximately 50% are implementing due to increasing security threats and DNSSEC industry awareness.*

a. If the registry is a sponsored TLD, what were the nature and content of these consultations with the sponsored TLD community?:

Not Applicable

b. Were consultations with gTLD registrars or the registrar constituency appropriate? Which registrars were consulted? What were the nature and content of the consultation?:

As previously described, Verisign has consulted with registrars over the past several years which consultations included: educational discussions about DNSSEC; solicitations of registrar and registrant interest; discussions around market demand for DNSSEC including registrar surveys/interviews to gauge demand; and discussion of what registrars need to facilitate a successful implementation. Most recently, these consultations included:

- *Registrar survey conducted during the summer of 2009 and 2010; and*
- *Information provided during Verisign-sponsored registrar events to:*
  - *Educate registrars on DNSSEC;*
  - *Advise registrars of Verisign's plan to sign .name*
  - *Gauge registrars' levels of interest and solicit their plans to include DNSSEC on their roadmaps:*
  - *Verisign's participation and communications on the topic of DNSSEC at*
    - *IETF Meetings*
    - *NANOG*
    - *ICANN meetings and updates to Registrars during the course of the DNSSEC Workshops*

Verisign, in cooperation with EDUCAUSE, implemented DNSSEC within the .edu zone for educational domain names in August 2010. EDUCAUSE is the sole registrar of the .edu name space. Prior to implementing DNSSEC, Verisign and EDUCAUSE deployed a testbed environment to engage members of the educational community. Verisign and EDUCAUSE interacted with 11 prominent educational organizations, to test our approach to DNSSEC and to obtain feedback on our approach and support materials. This approach allowed end-to-end testing by selected .edu domain holders in a non-production environment. This collaboration validated the implementation approach of starting with a smaller zone base and engaging .edu registrants to create technical awareness and to understand the registrars' implementation challenges.

c. Were consultations with other constituency groups appropriate? Which groups were consulted? What were the nature and content of these consultations?:

Verisign engaged with industry vendors and providers to communicate the impacts of DNSSEC prior to its implementation of DNSSEC in the .com and .net TLDs. Additionally, Verisign continues to present DNSSEC at industry trade events such as IETF, FOSE, and ICANN.

Root Zone: Verisign, in cooperation with ICANN's operations organization and the Department of Commerce, implemented DNSSEC at the root level of the DNS infrastructure in July 2010. The Deliberately Unvalidatible Root Zone (DURZ) rollout methodology was developed to create a "staged deployment" in order to incrementally introduce changes to the DNS root zone system. This best practice methodology allowed changes to be incrementally introduced, allowing the team and the broader Internet community to assess the impact of each change and ensure that the changes were visible to the community with no performance or functional impacts before proceeding to the next stage. Activating DNSSEC in the root paved the way for Internet TLDs to insert their signed records in the top of the DNS hierarchy, thereby creating the anchor of trust chain that DNSSEC requires in order to bring integrity to the entire system. The DURZ methodology and approach have been instrumental to introducing DNSSEC to the core of the internet infrastructure in an orderly fashion. This approach has been used successfully by other TLD operators.

Educational Name Space: As described above, Verisign worked with EDUCAUSE and the educational community for the implementation of DNSSEC.

d. Were consultations with end users appropriate? Which groups were consulted? What were the nature and content of these consultations?:

A significant body of anecdotal evidence has been discussed in public forums and among ICANN constituencies that support the value of the service; however, we have limited direct relationship with registrants of .name domains or other end users to appropriately document their views.

Verisign solicited feedback from the end-user registrants resulting from our work with EDUCAUSE in the DNSSEC test bed. We received positive and valuable feedback from the educational participants (registrants) of the test bed on our approach.

Additionally, Verisign engaged in a DNSSEC campaign in the first quarter of 2011 with the computer media organization CXO. The topic and technology were featured in banner ads for IT publications such as CIO, CFO, CSO and NetworkWorld. Verisign also gathered sentiment from readers of these periodicals through an online survey and poll on the topic. Relevant information has been shared at ICANN events.

In 2010, Verisign has also conducted DNSSEC research with Forrester and Frost & Sullivan to assess the community's interest and preparedness. The results are documented in white papers that reside on Verisign's DNSSEC web portal and webinars conducted in 2010:
http://verisigninc.com/en_US/why-verisign/innovation-initiatives/dnssec/additional-resources/index.xhtml

e. Who would endorse the introduction of this service? What were the nature and content of these consultations?:

Endorsement for the ecosystem wide introduction of DNSSEC is well documented through many public forums to include ICANN meetings. Additionally, the community has seen greater adoption of DNSSEC by registries in the past two years. Many public registries that manage country code TLDs and gTLDs have signed the zones that they operate with approximately ¼ of the zones in the Internet name space are signed.

f. Who would object the introduction of this service? What were(or would be) the nature and content of these consultations?:

While there is significant evidence of the value of DNSSEC in the authentication of DNS queries, not all registrants of domain names will elect to DNSSEC enable their own records due to a host of reasons.

DNSSEC will be offered to all registrars as an opt-in, value-add service. Each registrar may implement DNSSEC based on considerations such as demand from its customer base, budget and technical roadmap. Verisign will encourage adoption by supporting all registrars with tools and communications, including a modified EPP SDK and Tool enabled for DNSSEC and an operational test environment for the registrars to test their DNSSEC-enabled application prior to deployment. Based in part on this approach, Verisign does not anticipate any objections.

Timeline

Please describe the timeline for implementation of the proposed new registry service:

Verisign intends to implement the DNSSEC functionality in the .name TLD by Q3 2013.

Prior to implementing DNSSEC in the .name TLD and in order to support and encourage registrar implementation of DNSSEC, Verisign will provide registrars with the following:

o Educational information, technical support and technical seminars;
o Technical implementation documentation and tools that Verisign has made available to registrars as a result of the implementation of DNSSEC in .net and .com as noted above.

o Product deployment notification; and
o An Operational Test Environment for registrars to test their systems' DNSSEC functionality prior to deployment into the production environment.

Business Description

Describe how the Proposed Service will be offered:

Verisign will make DNSSEC available to all ICANN-accredited registrars as an opt-in, value-add service. Registrars will be encouraged, but not required, to offer DNSSEC functionality to both the new and existing .name domain names they manages on behalf of registrants. Registrars will be able to add/delete/modify registrant signed data into the registry utilizing systematic changes through EPP or through Verisign's web-based customer console. Verisign will not charge for DNSSEC.

Interface to the Registry

Registrars utilize the Extensible Provisioning Protocol (EPP) to process changes in the .name registry. Permissible changes include adding and deleting domain names and name servers, and changing the name servers associated with a domain name. When the .name zone is signed, registrars will also have the ability to communicate its registrants' DNSSEC key material to Verisign. This key material takes the form of Delegation Signer (DS) records, which will appear in a signed .name zone..

EPP has been extended to support DNSSEC: the Domain Name System (DNS) Security Extensions Mapping for the
Extensible Provisioning Protocol specification is defined in RFC 5910; J. Gould et al. (Verisign); May 2010. As part of DNSSEC-enabling the .name zones, Verisign's registry system will allow addition or deletion of DS records related to the domains over EPP. All EPP operations that are currently available will continue to be supported.

Resolution of DNSSEC enabled names

The .name zone is hosted entirely on Verisign's DNS platform. Verisign is enabling DNSSEC support within this environment to resolve signed names within the .name top level domain.

Signing & Key Rollover

Verisign will generate and hold all keys (both Key Signing Key (KSK) and Zone Signing Key (ZSK)) for the .name zone using a hardware security module (HSM) certified at FIPS 140-2. All signing operations will therefore occur inside the HSM.

The .name zone will be signed with NSEC3 and its Opt-Out feature (both documented in RFC 5155) using the RSA and

SHA256 algorithms (specifically DNSSEC algorithm number 8, RSA/SHA-256.

Delegation Signer (DS) and NSEC3 resource record sets (RRSets) will use signature duration of seven (7) days. DS RRSets will have a time to live (TTL) value of one day and NSEC3 records will have a TTL of 15 minutes (the same value as the SOA MINIMUM field, as specified by RFC 5155). While these values specify the initial configuration parameters, Verisign may modify the values as necessary to support industry standards, best practices, or operational requirements.

KSK - The KSK will be a 2048 bit key. The KSK will be used for a year at a minimum. After the first year, Verisign will annually assess the viability of the key based on current cryptanalysis techniques and only roll the KSK when it becomes necessary.

ZSK - The ZSK will be a 1024 bit key. The frequency for key rollover will be four times per year.

Describe quality assurance plan or testing of Proposed Service:

Verisign will conduct internal testing of the .name registry system to verify the functionality and performance with DNSSEC-enabled domain names.

The primary goal of the testing is to exercise the registration and resolution systems in Verisign's test environments, by managing the DS record provisioning for test names and querying DNS for the registered test names in Quality Assurance and Performance and Scalability environments. Specifically, Verisign will be conducting internal testing of its registration a resolution platform to:

o Demonstrate that all the components involved in signing .name domains are functioning properly;
o Document any points at which the expected behavior differs from actual behavior; and
o Measure the throughput and performance of the provisioning platform, updates to the name server constellation and resolution of the names in the testing environment to verify that DNSSEC can be introduced without impact to Verisign's service level agreements.

This end-to-end testing will ensure that all involved systems are functioning correctly, including:

o Registrar to Registry EPP protocol application; and
o Zone file updates.

Verisign operates the .name domain registration platform, in addition to the .com and .net domain registration platforms and manages the technical operations of the .edu Top Level Domain. In addition to signing for the second domain level, .name will be signed for the third domain level and for MX records to support its email forwarding service.

Verisign will leverage the testing approach and deployment methodologies that it applied when deploying DNSSEC in the .com, .net, and .edu zones. Verisign will leverage this experience and lessons learned from the earlier deployments and apply it to securing the .name space with DNSSEC security extensions.

Please list any relevant RFCs or White Papers on the proposed service and explain how those papers are relevant.:

The following RFC's were referenced and are being leveraged to support Verisign's implementation of DNSSEC in the .name space.

o RFC #4033 - DNS Security Introduction and Requirements - a description of DNSSEC and its capabilities and limitations
o RFC #4034 - Resource Records for the DNS Security Extensions - the introduction of new DNS resource record types:
o DNS Public Key (DNSKEY), Resource Record Signature (RRSIG), Next Secure (NSEC) and Delegation Signer (DS)
o RFC #4035- DNSSEC Protocol Modifications - which defines the concept of a signed zone, along with the requirements for serving and resolving by using DNSSEC
o RFC #5155 - DNS Security (DNSSEC) Hashed Authenticated Denial of Existence - use of an alternative resource record,
o NSEC3, which provides for incremental additions of DNSSEC signed data to signed zones
o RFC #5910 - Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)-utilizing the EPP mapping for the provisioning and management of Domain Name System security extensions (DNSSEC) for domain names stored in a shared central repository
o Verisign DNSSEC and Domains Transfers paper, March 2010, which can be located at:
http://www.verisigninc.com/assets/whitepaper-dnssec-transfers.pdf

Contractual Provisions

List the relevant contractual provisions impacted by the Proposed Service:

Section 3.1(c)(i) Data Escrow of the Registry Agreement. In addition Appendix 1 to the Registry Agreement would need to be updated to reflect the inclusion of DNSSEC Data.
No other contractual provisions will be impacted. The implementation specifications have been defined in an EPP extension published by Verisign for registrars and will be made available in advance of deployment on the registrar section of the registry website.

What effect, if any, will the Proposed Service have on the reporting of data to ICANN:

None.

What effect, if any, will the Proposed Service have on the Whois?:

None. The WHOIS RFC does not specify if, how, or what DNSSEC data should be displayed. Broader adoption of DNSSEC may yield best practices for including DNSSEC data in WHOIS, at which time Verisign will revisit this issue.

Contract Amendments

Please describe or provide the necessary contractual amendments for the proposed service:

The first two sentences of Section 3(c)(i) would be amended to read as follows:

Data Escrow. Registry Operator shall establish at its expense a data escrow or mirror site policy for the Registry Data compiled by Registry Operator. Registry Data, as used in this Agreement, shall mean the following: (1) data for domains sponsored by all registrars, consisting of domain name, server name for each nameserver, registrar id, updated date, creation date, expiration date, status information, and DNSSEC delegation signer ("DS")(if Registry Operator implements DNSSEC); (2) data for nameservers sponsored by all registrars consisting of server name, each IP address, registrar id, updated date, creation date, expiration date, and status information; (3) data for registrars sponsoring registered domains and nameservers, consisting of registrar id, registrar address, registrar telephone number, registrar e-mail address, whois server, referral URL, updated date and the name, telephone number, and e-mail address of all the registrar's administrative, billing, and technical contacts; (4) domain name registrant data collected by the Registry Operator from registrars as part of or following registration of a domain name; and (5) DNSSEC resource records in the zone (if Registry Operator implements DNSSEC).

Benefits of Service

Describe the benefits of the Proposed Service:

Verisign believes that introduction of DNSSEC functionality in the .name registry and resolution systems will benefit the Internet community by improving the security for the .name domain space and decreasing the likelihood that Internet users are subject to "man in the middle" and cache poisoning attacks.

Competition

Do you believe your proposed new Registry Service would have any positive or negative effects on competition? If so, please explain.:

Verisign believes that the implementation of DNSSEC into the .name registry systems is needed to improve the security of the Internet infrastructure as a whole, will enhance the protection services currently offered in the market place, allow registrars to market a new service related to domain names, better enable registrars to differentiate their services and compete more effectively, and give consumers more choices thereby enhancing competition.

How would you define the markets in which your proposed Registry Service would compete?:

DNSSEC will also be attractive to registrants interested in (i) improving the security features related to their online presence; and (ii) providing additional layers of trust to their customers.

What companies/entities provide services or products that are similar in substance or effect to your proposed Registry Service?:

Verisign, as the registry operator for the .name domain space, is the only operator capable of implementing DNSSEC functionality for the .name domain names.

The Internet community has seen greater adoption of DNSSEC by registries in the past two years. Nearly 90 registries that manage country code TLDs and gTLDs have signed the zones that they operate.

In view of your status as a registry operator, would the introduction of your proposed Registry Service potentially impair the ability of other companies/entities that provide similar products or services to compete?:

No. The registry operators for the TLD listed above currently provide similar services within other registry's respective TLDs. Signing the .name zone can only be offered by the .name registry operator.

Do you propose to work with a vendor or contractor to provide the proposed Registry Service? If so, what is the name of the vendor/contractor, and describe the nature of the services the vendor/contractor would provide.:

No.

Have you communicated with any of the entities whose products or services might be affected by the introduction of your proposed Registry Service? If so, please describe the communications.:

Yes. In addition to the communication and survey with the registrars, Verisign has implemented an interoperability lab for hardware vendors to review their equipment with DNSSEC enabled domain names. Verisign has also been engaged with the Hardware/networking Community through the introduction of a DNSSEC Interoperability Lab since December 2009. The Verisign DNSSEC Interoperability Lab helps alleviate vendors' DNSSEC-related concerns by allowing the Internet community to test network hardware and software in a standalone DNSSEC-enabled environment. The lab was free of charge and allowed hardware and software vendors to systematically identify and address product compatibility issues resulting from DNSSEC that may impact their customers and partners. At of the close of 2010, 8 industry-leading vendors have completed Interoperability Lab testing.

Do you have any documents that address the possible effects on competition of your proposed Registry Service? If so, please submit them with your application. (ICANN will keep the documents confidential).:

Verisign does not have any additional documents to submit.

Security and Stability

Does the proposed service alter the storage and input of Registry Data?:

The implementation of DNSSEC will allow Registrars to submit DS record data to the shared registry system as recommended in RFC 5910. Verisign's registry system will allow addition or deletion of DS records related to a .name domain over EPP in addition to the currently allowed operations.

Please explain how the proposed service will affect the throughput, response time, consistency or coherence of reponses to Internet servers or end systems:

Signed DNS records are significantly larger than the records of current, unsigned domain names. Once introduced into the registry system, the larger size, combined with the additional process oriented steps to sign the names within the zone, will likely cause the system to have a slightly increased throughput and potentially slower response times. However, in anticipation of this additional load, Verisign, is planning to conduct infrastructure wide upgrades to its shared registry and resolution platforms to minimize the impact of the significantly larger resource records. Therefore, Verisign does not anticipate that the additional size and processes to exceed the service level agreements in the current registry agreements.

Have technical concerns been raised about the proposed service, and if so, how do you intend to address those concerns?:

Verisign recognizes that the following concerns about DNSSEC may exist within the community:

o Understanding and complexity with signing domain names and managing key rollovers;
o The ability for older network equipment to receive and process the larger DNSSEC enabled queries.

Verisign has provided the registrar community with educational materials and an implementation guide sign and manage DNSSEC enabled domains. Additionally, Verisign did conduct internal testing of the registry systems to review the performance and scalability of the registry system and created an interoperability lab for networking vendors to test their equipment with DNSSEC-enabled domain names to support the deployment of DNSSEC for the .com, .net and .edu TLDs. Verisign believes this should be sufficient to support the deployment of DNSSEC for the .name TLD.

Other Issues

Are there any Intellectual Property considerations raised by the Proposed Service:

Verisign is not aware of any intellectual property considerations.

Does the proposed service contain intellectual property exclusive to your gTLD registry?:

(1) Trademark or similar rights may exist or arise with respect to trade names or terminology used in connection with the proposed service. (2) Copyright protection may exist or arise in connection with code written or materials created in connection with the proposed service. (3) Certain information or processes related to the service may be confidential to Verisign and/or subject to trade secret protection. (4) Verisign is not aware of the issuance of any patents by any party with respect to the service.

List Disclaimers provided to potential customers regarding the Proposed Service:

Verisign intends to include industry standard disclaimers, such as a disclaimer of all warranties, in the service agreement.

Any other relevant information to include with this request:

None.