ICANN Registry Request Service

Ticket ID: I7K6V-3R9C2
Registry Name: VeriSign, Inc,
gTLD: .COM, .NET, .NAME
Status: ICANN Review
Status Date: 2009-10-22 18:54:00
Print Date: 2009-10-22 18:54:04

Proposed Service

Name of Proposed Service:

DNSSEC - com and net

Technical description of Proposed Service:

Background:

DNS Security Extensions (DNSSEC) is a protocol for securing certain aspects of the Domain Name System. It is a set of extensions to DNS, which will provide end-to-end authenticity and integrity and protect the Internet from certain types of attacks.

VeriSign has always worked closely with the Internet community in the development of topics of Internet security including DNSSEC. VeriSign recognizes that Internet security is constantly evolving, and DNSSEC is one of many measures that are currently underway to enhance security on the Internet.

Internet Security

Many businesses already rely on VeriSign's public key infrastructure and digital certificates to secure their websites on the Internet, a serious responsibility that VeriSign works hard to maintain. VeriSign's DNSSEC strategy will leverage proven business processes and technical expertise to incorporate public key cryptography into the DNS hierarchy for the zones which it manages.

DNSSEC

VeriSign's research personnel have been, and continue to be, active participants in the technical community on DNSSEC and other security related improvements. In addition, VeriSign has made significant contributions towards shaping the standards which are being used by several registries currently deploying DNSSEC. VeriSign business personnel and the research labs have been engaged in DNSSEC for almost a decade. In fact, VeriSign has:

o Conducted thorough research related to DNSSEC by operating test beds in its VeriSign lab program;
o Taken an active role in discussions and working groups hosted by the IETF (i.e., Internet Engineering Task Force) and the DNSSEC Coalition;

o Worked collaboratively with other registries and IT security experts to evaluate the DNSSEC standards and co-author the newly adopted RFC related to the NSEC3 protocol addition; and
o Created an open and continuous dialogue with registrars in order to educate and encourage adoption and incorporation of DNSSEC into their environment

VeriSign proposes to implement DNSSEC functionality for the .net and .com top level domains in an effort to protect Internet users from forged DNS data. Implementation of DNSSEC technology will (i) fortify DNS data for the Internet community, thereby guarding against situations in which its integrity may be compromised; and (ii) assist in protecting the .com and .net top level domains from 'man in the middle attacks" and/or cache poisoning in recursive name servers.

Technical Description:

VeriSign will introduce DNSSEC functionality into the .com and .net registries by modifying its current EPP implementation. More specifically, VeriSign will modify the EPP interface between VeriSign, as the registry operator for the .com and .net top level domains, and the registrars so that registrars can submit DS record data through the interface as defined in RFC 4310: The Domain Name System Security Extensions Mapping for the Extensible Provisioning Protocol. VeriSign intends to provide an Operational Test Environment ("OTE") which has been configured to accept DNSSEC records for use by all registrars prior to implementing the new functionality in its production environment.

In addition, VeriSign intends to:

o Implement DNSSEC in accordance with relevant RFCs: 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 4310
o Provide all registrars with the ability to support DNSSEC for their registrants, and will have use cases available for Registrar to validate DNSSEC functionality.
o Evaluate the need and benefit of modifying Whois to reflect DNSSEC signed domain names. (Note that at this time, Whois modifications are not expected).

Appendix A (DNSSEC-RSEP-attachment.pdf)

Appendix B (DNSSEC-RSEP-attachment.pdf)

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:
? RFC #4033 - DNS Security Introduction and Requirements; Matt Larson (VeriSign), et al., March 2005
? RFC #4034 - Resource Records for the DNS Security Extensions; Matt Larson (VeriSign), et al., March 2005
? RFC #4035 - DNSSEC Protocol Modifications; Matt Larson (VeriSign), et al., March 2005
? RFC #5155 - DNS Security (DNSSEC) Hashed Authenticated Denial of Existence; David Blacka (VeriSign), et al., March 2008
? RFC #4310 - Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP); S. Hollenbeck (VeriSign); November 2005

In the past year, VeriSign has engaged with the registrar community on the topic of DNSSEC. VeriSign has learned that DNSSEC knowledge and experience vary widely among registrars. A survey conducted in the summer of 2009 identified that a better understanding of the registry to registrar interface, a clear value proposition and more training and technical information on the topic of DNSSEC would be of value to the registrars. VeriSign is enclosing the results of the survey as an attachment.

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:
o Registrar survey conducted during the summer of 2009; and
o Information provided during VeriSign-sponsored registrar events to:
o Educate registrars on DNSSEC;
o Advise registrars of VeriSign's plan to sign .net and .com
o Gauge registrars' levels of interest and solicit their plans to include DNSSEC on their roadmaps
VeriSign is currently working with EDUCAUSE, the sole registrar of the .edu name space, to methodically test and deploy DNSSEC into the .edu zone. VeriSign has provided technical tools and guidance to EDUCAUSE on the registry to registrar interface by providing a software development tool kit and a tool to evaluate EPP responses to DNSSEC data. VeriSign will make these tools and support documents available to the registrars implementing DNSSEC in the .com and .net name space

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

VeriSign has initiated discussions with network providers and 3rd party vendors who are expected to be impacted by the implementation of DNSSEC. Additionally, VeriSign has worked with the IETF for the formation of the current standards related to DNSSEC standards as described above.

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 .com and .net domains or other end users to appropriately document their views.

We have identified significant support by .edu registrants through our work with Educause.

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.

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 a 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 .net TLD by Q4 2010 and in the .com TLD by Q1 2011.

Prior to implementing DNSSEC in the .com and .net TLDs 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. (Note that VeriSign has already made some of these tools available to registrars, including VeriSign's EPP Software Development Kit (SDK) which has been available to registrars since December 2008, and the EPP Tool which was recently updated to include DNSSEC support. VeriSign will continue to provide registrars with additional documentation, guides and tools to support their implementation and key management.
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 .com and .net 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 .com and .net registries. Permissible changes include adding and deleting domain names and name servers, and changing the name servers associated with a domain name. When the .com and .net zones are 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 .com and .net 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 4310; S. Hollenbeck (VeriSign); November 2005. As part of DNSSEC-enabling the .com and .net 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 .net and .com zones are hosted entirely on VeriSign's DNS platform. VeriSign is enabling DNSSEC support within this environment to resolve signed names within the .com and .net top level domains.

Signing & Key Rollover

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

The .net and .com zones will be signed with NSEC3 and its Opt-Out feature (both documented in RFC 5155) using the RSA and SHA1 algorithms (specifically DNSSEC algorithm number 7, RSA-NSEC3-SHA1).

Delegation Signer (DS) and NSEC3 resource record sets (RRSets) will use a 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 .com and .net registry systems 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 and resolution platforms to:
o Demonstrate that all the components involved in signing .com and .net 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;
o Zone file updates; and
o DNS resolution in the test environment.

VeriSign operates the .com and .net domain registration platforms, and manages the technical operations of the .edu Top Level Domain. The .edu zone leverages many of the same implementation practices and connection protocols that are used for the .com and .net domain space. The .edu TLD systems are functionally equivalent to VeriSign EPP code base and implementation for the .net and .com TLDs.

VeriSign is in the process of deploying DNSSEC in the .edu zone with the sole registrar, EDUCAUSE, and a select number of test registrants in 2009. This test bed will enable VeriSign to conduct end-to-end testing of DNSSEC-enabled names in a non-production environment. The test results obtained through collaborative testing will provide VeriSign with information and data on the code base and business processes that VeriSign intends to leverage to sign the .net and .com zones.

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 .com and .net 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: 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, NSEC3, which provides for incremental additions of DNSSEC signed data to signed zones
o RFC #4310 - 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

Contractual Provisions

List the relevant contractual provisions impacted by the Proposed Service:

No contractual provisions will be impacted. The implementation specifications have been defined in an EPP extension published by VeriSign for registrars and currently available 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.

ICANN Registry Request Service

Ticket ID: I7K6V-3R9C2
Registry Name: VeriSign, Inc,
gTLD: .COM, .NET, .NAME
Status: ICANN Review
Status Date: 2009-10-22 18:54:00
Print Date: 2009-10-22 18:54:04

Contract Amendments

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

No contractual amendments will be required

Benefits of Service

Describe the benefits of the Proposed Service:

VeriSign believes that introduction of DNSSEC functionality in the .com and .net registry and resolution systems will benefit the Internet community by improving the security for the .com and .net 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 .com and .net 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 .net and .com domain space, is the only operator capable of implementing DNSSEC functionality for the .net and .com domain names.

The following gTLD's are currently signed and will be offering second level DNSSEC domain signatures:
o .gov;
o .org
o .museum

The following country code TLD's operate a signed zone:
o Brazil (.br)
o Bulgaria (.bg)
o Czech Republic (.cz)
o Puerto Rico (.pr)
o Sweden (.se)

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 TLDs listed above currently provide similar services within their respective TLDs. Signing the .net and .com zones can only be offered by the .com and .net 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 is pursuing an interoperability lab for hardware vendors to review their equipment with DNSSEC enabled domain names.

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.

ICANN Registry Request Service

Ticket ID: I7K6V-3R9C2
Registry Name: VeriSign, Inc,
gTLD: .COM, .NET, .NAME
Status: ICANN Review
Status Date: 2009-10-22 18:54:00
Print Date: 2009-10-22 18:54:04

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 4310. VeriSign's registry system will allow addition or deletion of DS records related to a .net and .com 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 intends to provide the registrar community with educational materials and an implementation guide sign and manage DNSSEC enabled domains. Additionally, VeriSign will be conducting internal testing of the registry systems to review the performance and scalability of the registry system and creating an interoperability lab for networking vendors to test their equipment with DNSSEC-enabled domain names.

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.

ICANN Registry Request Service

Ticket ID: I7K6V-3R9C2
Registry Name: VeriSign, Inc,
gTLD: .COM, .NET, .NAME
Status: ICANN Review
Status Date: 2009-10-22 18:54:00
Print Date: 2009-10-22 18:54:04

Appendix {A(DNSSEC-RSEP-attachment.pdf)
(Seen on Next Page)

Registrar Feedback

- **Few registrars currently offer DNSSEC. Interest in offering a DNSSEC service to customers in the next 12 months is mixed.**

	Total Registrars	Top 20	Non Top 20	North America	Asia Pacific	Europe/ UK
	(56) %	A (9) %	B (47) %	C (29) %	D (9) %	E (15) %
Already Offer	5	-	6	10	-	-
Extremely/Very Likely to Offer	14	-	17	10	33	13
Somewhat Likely	38	44	36	38	22	40
Not Very/Not at all Likely to Offer	36	44	34	31	45	40
Don't know	7	12	7	11	-	7

- **Features That Would Make DNSSEC More Valuable**
  - 56 total interviews were conducted among registrars during June/July, 2009 (45% of Top 20 registrars and 13% of Non Top 20 registrars participated)

	Total Registrars
	(56)
Information on how the interface to the registry will accommodate DNSSEC	64 %
A clear value proposition	62 %
More training and tools for implementation	57 %
More technical information and guidance on how DNSSEC works	55 %
Marketing and messaging communications to use with your customers	50 %
The registry provides DNSSEC implementation services and support for a fee	34 %
Other*	5 %
Nothing, just not interested in offering	5 %
None	9 %

ICANN Registry Request Service

Ticket ID: I7K6V-3R9C2
Registry Name: VeriSign, Inc,
gTLD: .COM, .NET, .NAME
Status: ICANN Review
Status Date: 2009-10-22 18:54:00
Print Date: 2009-10-22 18:54:04

Appendix {B(DNSSEC-RSEP-attachment.pdf)
(Seen on Next Page)

Registrar Feedback

- **Few registrars currently offer DNSSEC. Interest in offering a DNSSEC service to customers in the next 12 months is mixed.**

	Total Registrars	Top 20	Non Top 20	North America	Asia Pacific	Europe/ UK
	(56) %	A (9) %	B (47) %	C (29) %	D (9) %	E (15) %
Already Offer	5	-	6	10	-	-
Extremely/Very Likely to Offer	14	-	17	10	33	13
Somewhat Likely	38	44	36	38	22	40
Not Very/Not at all Likely to Offer	36	44	34	31	45	40
Don't know	7	12	7	11	-	7

- **Features That Would Make DNSSEC More Valuable**
  - 56 total interviews were conducted among registrars during June/July, 2009 (45% of Top 20 registrars and 13% of Non Top 20 registrars participated)

	Total Registrars
	(56)
Information on how the interface to the registry will accommodate DNSSEC	64 %
A clear value proposition	62 %
More training and tools for implementation	57 %
More technical information and guidance on how DNSSEC works	55 %
Marketing and messaging communications to use with your customers	50 %
The registry provides DNSSEC implementation services and support for a fee	34 %
Other*	5 %
Nothing, just not interested in offering	5 %
None	9 %