ICANN Registry Request Service

Ticket ID: Z8J3W-7W5W3
Registry Name: NeuStar, Inc.
gTLD: .BIZ
Status: ICANN Review
Status Date: 2009-10-19 14:10:57
Print Date: 2009-10-19 14:11:00

Proposed Service

Name of Proposed Service:

DNSSEC in .BIZ

Technical description of Proposed Service:

The DNS Security Extension Protocol (DNSSEC) was developed to secure and protect DNS servers from a weakness identified fifteen years ago by the Defense Advanced Research Agency (DARPA). The original design of the Domain Name System (DNS) was intended to support a scalable, distributed system, but it did not include adequate security safeguards for the 21st century Internet. As an unintended result, the DNS was left vulnerable to abuse.

Following this discovery, DARPA sponsored research to find a way to make it difficult or impossible for a DNS server to be fooled by a forged message. ISPs run DNS servers as part of the service for their customers, if a DNS server has incorrect information as a result of a forged message the assets involved in e-commerce are at risk. Following the development of DNSSEC, the U.S. government (today DHS) funded efforts to deploy DNSSEC throughout the global public internet. Over time, DNSSEC had been thought to be too much security for everyday use until the US CERT issued advisory VU-800113 which identified a credible threat to the safety of DNS data. At that point, DNSSEC came to the forefront of Internet Security. Neustar believes that now is the right time to implement and support DNSSEC for the .BIZ gTLD.

DNSSEC was designed to protect Internet resolvers (clients) from forged DNS data, such as that created by DNS cache poisoning. Through such cache poisoning, those vulnerabilities are today being exploited. The development and implementation of DNSSEC adds security while maintaining backwards compatibility to the original design. All DNS answers incorporating DNSSEC are digitally signed, and by checking the digital signature, a DNS resolver is able to verify whether the information is identical to the information on the authoritative DNS server.

As stated in our response to the U.S. Department of Commerce's October 2008 Notice of Inquiry on DNSSEC, Neustar supports deployment of DNSSEC at the root zone level to ensure improved stability and security of the entire Domain Name System. Because signing of the root zone is not yet complete, we believe it is incumbent upon existing TLD registry operators to sign their respective TLD zones as an interim step. Neustar began supporting DNSSEC for TLD customers of our DNS hosting services in December 2008. That is, where Neustar provides primary or secondary DNS to an existing TLD registry operator, that registry operator is able to implement TLD-level DNSSEC while utilizing our DNS services. We intend to support DNSSEC for our TLD registry operations in 2009 and enterprise customers of our DNS hosting services in 2010.

Until the root zone is signed, the TLD registry operator must make the TLD public key (a Secure Entry Point in DNSSEC terminology) available via secure or verifiable means. Merely placing the public key on a WWW site is not by itself sufficient, so Neustar is working with the DNS community to determine the most reliable means to do this. Possible options for publishing keys include placing an advertisement in a widely read newspaper or periodical and utilizing Trust Anchor Repositories once they have proven to be reliable. Several other TLD registry operators have already signed their zones, including .SE (Sweden) and .CZ (Czech Republic), .BR (Brazil), .PR (Puerto Rico), .BG (Bulgaria) with many others in progress (.ORG, .NZ, .MUSEUM). Once the root zone is signed, .BIZ will transition to rely upon the signed root zone.

Technical Description of the Proposed Service
Neustar, Inc. requests authorization from the Internet Corporation for Assigned Names and Numbers (ICANN) for implementation of DNS Security Extensions (DNSSEC) at the .BIZ TLD level. A signed .BIZ zone will increase DNS security and allow .BIZ registrars to test and implement DNSSEC in advance of a signed root zone.

Neustar's DNSSEC implementation for the .BIZ gTLD zone will comply with the DNSSEC definitions in RFC 4033, RFC 4034, and RFC 4035 plus amendments to those documents reviewed and accepted by the IETF and published as subsequent RFCs. In particular, initially the .BIZ gTLD zone will use the NSEC option for negative answers, and the RSA/SHA-1 cryptographic algorithm.

The first public phase of DNSSEC operations will consist of signing the .BIZ zone. Subsequently we will include secured delegations for select registrations. Full operational capability will allow all registrants (working through registrars) to submit DNSSEC material via an interface supporting RFC 4310, EPP extensions for DNSSEC. Changes to the zone will continue to be made via dynamic update (RFC2136).

To enable registrar uptake of this opt-in service, Neustar will implement a backwards-compatible change to our registrar EPP client. The change will include a modification to allow manipulation of DNSSEC DS records by each participating registrar. Neustar's changes will be in compliance with RFC 4310.

To fully implement DNSSEC in .BIZ, Neustar's will:

o Make the production changes in the OT&E environment in advance of the production system changes.

o Recommend that participating registrars complete a DNSSEC OT&E test prior to use in the production environment.

o Make changes to the .BIZ nameservers to answer queries that request DNSSEC data for validation of the response.

o Neustar will self-sign the .BIZ zone initially. Once the root zone is signed, Neustar will deliver DS records for proper DNSSEC delegation in the root.

o Neustar will provide a report to registrars identifying which domain names are signed, along with their expiration time stamp.

o Neustar will not charge an additional registrar fee for support of DNSSEC.

Consultation

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

See below.

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?:

Neustar has not consulted with gTLD registrars or the registrar constituency. Because DNSSEC in .BIZ will follow several RFCs and will be offered as a voluntary, opt-in service, Neustar determined that registrar consultations were unnecessary. In 2004 and 2005 Neustar did conduct a trial of DNSSEC in the .US ccTLD and opened participation to all registrars, most of whom are also accredited by ICANN for .BIZ. Once DNSSEC has been approved and implemented at the registry level, Neustar will engage with registrars and the registrar constituency to help educate on the benefits of DNSSEC and to encourage registrars to support and promote it to their registrant customers.

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

Neustar has not consulted with other constituency groups.

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

Neustar has not consulted directly with end users.

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

The ICANN Board has already approved an identical service in two other gTLD (.ORG, and .MUSEUM).

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

Neustar is unaware of any opposition to the introduction of this service. Neustar looks forward to reviewing any concerns raised during the public comment period once this proposal is posted.

Timeline

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

Neustar intends to sign the .BIZ TLD zone by the end of 2009.

Our rollout plan is comprised by the following milestones:

o Complete development and testing of the EPP extensions and business policy rules to enable registrars and registrants to interact with the .US registry. (Completed in Q2 2009)

o Complete development and testing of DNSSEC extensions for dynamic publishing of DNSSEC resource records. (Completed in Q2 2009)

o Deployment of the SRS to OT&E enabling registrars to implement and test DNSSEC (To be completed +30 days from approval)

o Thorough testing of key management (including key lifecycle and APEX Keys), signature maintenance (including explicit updates and implicit re-signing activities). (Completed in Q2 2009)

o Establishment of a secure entry point public key in lieu of a signed root. We plan to interact with IANA for this. We will comply with RFC 5011 for changing secure entry points. (Will be completed approximately 30 days after zone signing)

We expect to be able to sign the zone in production shortly after we receive approval. This will entail a very controlled and deliberate path to ensure the continuing stability of the .BIZ gTLD zone.

o We will publically announce that we will begin to sign the root zone after approval and prior to the initial signing.

o The initial signing will not be announced and any statements regarding the activity will warn against placing reliance on the Secure Entry Point (SEP) (KSK) until we are satisfied that the migration is successful. (Will be completed approximately 30 days after signing)

o We will then publicly announce our signed zone and publish the keys through our secure website and validated trust anchors such as IANA. (Approximately 30 days after signing)

o Allow for a relatively small number of signed delegations in a "friends and family" mode. (Approximately 60 days after signing)

o With successful "friends and family" results, open up full participation to registrars. (Approximately 120 days after initial signing)

NOTE: This proposed timeline is for planning purposes only and is subject to change.

Business Description

Describe how the Proposed Service will be offered:

Business Description:

Neustar has invested significant resources to ensure our hardware, software and connectivity are architected and tested to ensure the highest levels of performance and DNS security. Neustar views the implementation and support for DNSSEC as a requirement for any world-class registry. Neustar does not view DNSSEC as a new business opportunity; rather, we consider it a requirement to ensure and maintain confidence in the DNS. Neustar will not seek to recoup our cost of implementing DNSSEC through increased fees to registrars.

Describe how the Proposed Service will be offered:

NeuStar will implement DNSSEC and will support DS records at the registry using EPP as described in RFC 4310. Once the .BIZ zone is signed and Neustar publishes our public key, participating .BIZ registrars will then be able to offer enhanced DNS security to their customers - the registrants of second-level .BIZ domain names.
Registrars will be encouraged to participate in a DNSSEC OT&E trial before implementing in production. Once Neustar publishes our public key, registrars and name server administrators will be alerted and provided with several sources to obtain the key, which will then be loaded into their respective nameserver infrastructures.

o Scheduled Key Roll-Over

For ZSKs, actions will occur on the 8th, 15th, and 22nd of each month. On the 8th a new key pair will be generated and placed into the DNS. On the 15th the current private key will be replaced by the next key. On the 22nd the exiting public key will be removed from the DNS. These steps are designed to run according "to calendar" for the sake of predictability. With a 6 day TTL, a 7 day interval is sufficient. The first of the month is avoided to allow it to be used for KSK operations and to avoid "new month issues." If there is an error, the 29th is available (or 28th for non-leap Februaries) to catch up. NeuStar reserves the right to amend or adjust these dates following implementation.

For KSKs, actions will happen on the first of the month in which an action is needed, and assumes an annual cycle. In March a new key is generated and the public key is put in DNS. In April a request is made of IANA to register the DS record (without a signed root, the repositories are notified). By May confirmation of the change is expected and the outgoing key is RFC 5011 marked as revoked. In June the revoked key is removed.

These plans are based on a draft under discussion see (http://tools.ietf.org/html/draft-morris-dnsop-dnssec-key-timing-00) in the IETF with a few simplifying assumptions. We will always carry an "emergency" key in the DNS so the loss of a key can be simply processed. All operations are scripted (except dealing with the unspecified IANA interface).

o Emergency Key Rollover

Emergency key rollover processes vary by kind of key and the phase of key management. The basic principle is to run through the normal steps of a key change in one move. For ZSK this means, generate, change the private key and then later

remove the broken key's public entry from the DNS in due time. For KSK, generate, request IANA change (or the repositories), revoke and then remove.

o KSK Compromise

KSK compromise is described above.

o Revocation of DNSSEC in the .BIZ gTLD

Revocation of DNSSEC will be supported by choosing a set of slave DNS servers that will maintain an unsigned version of the signed zone. In case of a need to drop DNSSEC, the unsigned zones will be loaded and then propagated to other servers. (Other servers will have been "pulled" from the network.) In addition, IANA and any repositories will be notified to remove the SEP material (e.g., DS record).

Describe quality assurance plan or testing of Proposed Service:

In 2004, Neustar conducted the first of two registry-registrar DNSSEC trials to test the use of the Extensible Provisioning Protocol (EPP). Neustar built technology that extended the registry EPP interface to include the passing of keys from a registrar to the registry. Subsequently, these keys were used to provision a special trial DNS service instance which was able to be queried in a lab environment. Based on lessons learned in past tests, new maturity in tools and ever growing threats of the DNS fabric Neustar moved DNSSEC back into a testing environment to ensure the latest versions of BIND can fully support DNSSEC and the exchanging of keys.

As we move from an internal testing environment to Operational Testing and Evaluation (OT&E), registrars will be able to connect to the registry and exchange data to ensure they have their code set up correctly. This is an opt-in and voluntary process, but one that every registrar will be recommended to follow before introducing DNSSEC in production.

The underlying registry implementation will feature options intended for potential future introductions in the .BIZ gTLD, such as NSEC3 support (RFC 5155), as well as other cryptographic options. These options include algorithms other than RSA/SHA1 which are available but not in use, as well as different key lengths. For example, DSA is available, defined, and included in openssl, but we have no current plans to make use of it in our .BIZ gTLD deployment.

Our testing to date has shown that support of DNSSEC for the .BIZ gTLD zone will require more powerful hardware (a larger class of server) and greater network capacity will be consumed. This does not affect our ability to meet contractual SLAs, but it has increased costs to the registry. Neustar will not pass on those incremental costs to registrars and registrants.

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

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

Neustar's DNSSEC implementation for the .BIZ gTLD zone will comply with the DNSSEC definitions in RFC 4033, RFC 4034, and RFC 4035 plus amendments to those documents reviewed and accepted by the IETF and published as subsequent RFCs. In particular, initially the .BIZ gTLD zone will use the NSEC option for negative answers, and the RSA/SHA-1 cryptographic algorithm. The first public phase of DNSSEC operations will consist of signing the .BIZ zone. Subsequently we will include secured delegations for select registrations. Full operational capability will allow all registrants (working through registrars) to submit DNSSEC material via an interface supporting RFC 4310, EPP extensions for DNSSEC. Changes to the zone will continue to be made via dynamic update (RFC2136).

Neustar's key management plan governing the use of DNSSEC's keys is derived from practices described in a collection of the US NIST Special Publications 800 Series. SP800-53, Recommended Security Controls for Federal Information Systems and Organizations, provides recommended security practices, whether or not applied to US Federal applications or something more general (as the BIZ gTLD is). SP800-57 part I and SP800-57 part 2, Recommendation for Key Management, provides recommendations for the handling and preparation of keys. In addition to this, we are consulting FIPS 140-2, Security Requirements for Cryptographic Modules, to determine the most appropriate level of compliance for the .BIZ gTLD.

Contractual Provisions

List the relevant contractual provisions impacted by the Proposed Service:

Section 3.1(c)(i) Data Escrow of the Registry Agreement (8 December 2006) between ICANN and Neustar.

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

Neustar does not anticipate DNSSEC implementation will create any changes to our reporting of data to ICANN.

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

At this time, Neustar does not intend to modify Whois to reflect DNSSEC, so there will be no effect on Whois.

Contract Amendments

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

EXISTING LANGUAGE

3.1 (c)(i) 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 related key material (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) the DNSSEC-related material necessary to sign the .biz zone (e.g., public and private portions of .biz zone key-signing keys and zone-signing keys)(if Registry Operator implements DNSSEC).

PROPOSED LANGUAGE

3.1(c)(i) 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 DS data (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).

ICANN Registry Request Service

Ticket ID: Z8J3W-7W5W3
Registry Name: NeuStar, Inc.
gTLD: .BIZ
Status: ICANN Review
Status Date: 2009-10-19 14:10:57
Print Date: 2009-10-19 14:11:01

Benefits of Service

Describe the benefits of the Proposed Service:

Implementation of DNSSEC will protect Internet resolvers (clients) from DNS cache poisoning by preventing the acceptance of forged data. The development and implementation of DNSSEC adds security while maintaining backwards compatibility to the original design. All DNS answers incorporating DNSSEC are digitally signed, and by checking the digital signature, a DNS resolver is able to verify whether the information is identical to the information on the authoritative DNS server. Implementing DNSSEC will ultimately help to ensure security and confidence in the DNS.

ISPs run DNS servers as part of their service to their customers, including Internet access, web hosting, email and other services. The corruption of zone data in these servers would result in putting e-commerce at risk and erode trust in the DNS and Internet. A specific benefit of DNSSEC provides the means for the receiver of a DNS message to authenticate the source of the message, i.e., the answer, is from the true source and not from a forger. It provides the means to verify that the complete answer is received, with no data added or removed, as well as protection against falsely indicating whether names are registered. The benefit of these features is that redirecting traffic from a legitimate site to another is not possible due "man in the middle attacks" and cache poisoning on DNS. Implementation of DNSSEC is one more step to a safe and secured internet.

Competition

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

Neustar believes the implementation of DNSSEC in .BIZ will have no impact on competition.

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

Neustar's implementation of DNSSEC in .BIZ may attract businesses (registrants) concerned with the DNS security.

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

o Public Interest Registry (PIR) in the .ORG domain.

o Musedoma in the .MUSEUM domain.

o The Internet Infrastructure Association, ccTLD Registry Operator of .SE

o NIC.CZ, ccTLD Registry Operator of .CZ.

o and others

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.

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, Neustar will not work with a vendor or contractor to implement DNSSEC in .BIZ.

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, Neustar personnel have been involved in the development of the DNSSEC protocol since its inception. We have also engaged in outreach efforts to raise awareness of DNSSEC and to advise carriers, hardware manufacturers, and software developers about the need for systems that will make appropriate use of DNSSEC.

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).:

Neustar anticipates signing the .BIZ zone will have no impact on competition.

Security and Stability

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

Neustar anticipates a change in the storage and/or input of Registry Data. As specified by RFC 4310, registrars will have the ability to enter and manipulate DNSSEC DS records via an extension to the EPP protocol.

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

Neustar anticipates no adverse impact on the throughput, response time, and consistency of coherence of responses to Internet servers or end systems. Neustar has invested in hardware and software and testing to ensure that our performance and SLAs remain within acceptable limits.

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

Neustar is not aware of any technical concerns regarding the proposed service.

Other Issues

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

No, there are no Intellectual Property considerations raised by the implementation of DNSSEC in the .BIZ gTLD.

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

No.

List Disclaimers provided to potential customers regarding the Proposed Service:

Not applicable.

Any other relevant information to include with this request:

Anticipated Questions from the RSTEP Review Team, as noted in the application for DNSSEC in .ORG, and Neustar's responses:

Please describe your policies on the following topics. If you have formal policy documents, please supply them; otherwise, please list whatever informal information you have on the Neustar policies for the topics listed.

P1. KSK key generation and storage

KSK key, or more accurately Secure Entry Point (SEP) key, generation will occur on the primary hidden master serving the BIZ zone. When a KSK is generated it is copied to the secondary hidden master, which runs in an active/active configuration. Once a KSK is generated the public half of the key is placed in the apex DNSKEY set of the zone and the key files (public and private) are placed where they can be used by the name server to sign the DNSKEY set.

The KSK key material is deleted after the key effectivity period of the KSK; this is anticipated to be 2 years (one year as an emergency key and one year as the active key). The KSK will be retired according to RFC 5011 rules.

P2. ZSK key generation and storage

ZSK key generation and storage is subject to the same steps as the KSK in P1, with the exception that the ZSK effectivity period is on the order of months, not years, and RFC 5011 does not apply to a non-SEP key.

P3. Zone signing - signature generation, RRSIG validity period, and resigning strategies

Beyond the initial conversion to DNSSEC, there is no "zone signing" per se as the zone is maintained in an incremental fashion due to its size and churn rate. For an individual RRSet, it will be signed as a result of a change or when the existing signature is in need of a refresh.

RRSIG records will have a signature expiration time 30 days into the future of the signature inception date. The target for resigning is 14 days. These times are chosen for clarity and a margin for error in operations. That is, if there is a problem with the signature generation activity on one day, there is still enough time to catch up and retain the 30 day cycle.

P4. Normal key rollover

Scheduled key supercession, or "rollover", will follow a monthly calendar for ZSKs and an annual calendar for SEP (KSK) keys.

Changing the ZSK key is done in three steps, involves three keys (new, emergency, active) and does not involve an external party.

The first step will occur regularly on a monthly basis (we plan on the 8th of the current month). The step will entail generating a new key pair and immediately publishing the public component in a DNSKEY RR in the zone. As we have a 6 day TTL, this publication happens 7 days before the next step to allow the new key to reach caches.

The second step entails moving the emergency key files into a directory where the name server will begin to use that key for new signature generation and removal of the files from the directory that correspond to the erstwhile active key. This step effectively changes the signing key.

The third step is the cleanup. The erstwhile active key is removed from the DNSKEY RR set as published in the zone. This step happens 7 days after the second step, and with a 6 day TTL all copies of signatures generated by this key will have been removed by compliant caches.

Changing the SEP (KSK) key is done in approximately the same manner but involves interaction with external parties causing step 2 above to be split into two pieces because we cannot predict the time needed for that interaction. As before there is a new key, an emergency key, and an active key involved. The active key is the key with a corresponding DS RR in the parent zone or in one or more Trust Anchor Repositories failing having a signed root zone.

The first step will occur on a regular annual basis (we envision March 1 as a time when these changes will have a lessened impact on our customers and relying parties) and each step will be given a 1 month time to complete so as to not conflict with ZSK supercession. The first step entails the generation of a new key and the placement of it in the DNSKEY set.

One month later, the second step will begin by placing the emergency key's files into the directory where the name server will begin to use the keys to sign the DNSKEY set. At this time a request will be made to "publicize" the emergency key as the new active key. The request should go to IANA as the root zone maintainer but there is no interface for this defined.

Knowing the issue of signing the root and putting that aside, there has been no hint about how IANA would accept DS records from the TLDs if they were proceeding with signing the root zone. In absence of a DNSSEC enabled parent zone we are forced to make use of Trust Anchor Repositories.

Allowing for a month to pass to ensure that the emergency key has replaced the active key as the SEP in whatever repositories we contact, the second half of the second step begins. In this half, the active key is marked as revoked in accordance with RFC 5011.

Another month passes to allow the revocation of the active key to be spread to all that want to know. At this point, in the third step, the active key is pulled from the DNSKEY set in the zone and its key files removed and destroyed.

P5. Emergency key rollover

An emergency key supercession (rollover) is more or less a compressed version of a 3 step scheduled supercession, collapsing all the steps into one. Once an active key is determined to be compromised, a new key is generated and pressed into service as the next emergency key, the current emergency key is promoted to active, and the active key retired, the details depend on whether the key is SEP or not.

An analysis of the scenarios does indicate that there are slight differences in the phases of the supercession (i.e., between step 1 and 2, 2 and 3, 3 and 1, etc.) but all essentially call for a compressed supercession. In one case the active period of a key is lengthened, that being the situation in which we are already preparing an emergency for a scheduled promotion but it is needed a short time earlier (a short time being less than the duration of the steps).

P6. Normal flow of data from child zone for creation of DS records

DS records are introduced to the registry, and thus the zone, via the EPP protocol per RFC 4310, Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol and are reflected automatically in the zone as for other EPP initiated changes.

P7. Emergency flow of data from child zone for creation of DS records

Emergency update of DS records is as described in P6, Normal flow of data from child zone for creation of DS records.

P8. Distribution of signed zone to authoritative servers

Signed zones will be distributed in precisely the same manner as unsigned zones, that is using IXFR [RFC 1995], NOTIFY [RFC 1996] and TSIG [RFC 2845]. The DNS interface to the registry (the "distributor") implements these protocols in order to

propagate zone changes out to distribution masters in each nameserver cluster.

P9. DNSSEC procedures for change of registry if the .BIZ TLD itself is changed to another organization

Nearly the entire burden of transitioning the .BIZ TLD to another organization would fall on the new registry provider. Since the KSK and ZSK information will not be escrowed, the new provider would need to generate keysets for both the KSK and ZSKs. Neustar would then add these keys, without signing the zone with them, prior to cut-over. At cut-over, the new organization would need to invoke a KSK key rollover per their procedures. All DS data sent by the registrars would be transitioned over to the new organization, as well as the zone data.

P10. Turning off DNSSEC if there are failures (and what thresholds would trigger such an action)

DNSSEC might disrupt Internet operations in a number of ways, and in ways we cannot anticipate. But to run through some foreseeable meltdown scenarios and reactions to them, here is a list.

DNSSEC records cause the slave name servers to terminate operations. The consequence of this is that the BIZ zone would be unavailable to the Internet. In anticipation of this, we will have a select number of slave servers maintaining a DNSSEC-stripped version of the BIZ zone on local disks. The local copy limits the mean-time-to-repair in this case. Upon detection that DNSSEC is somehow stopping our name servers we will load in the unsigned records and immediately request the DS records be pulled from Trust Anchor Repositories (this is a situation that a signed root zone with an good, automated interface would be a good thing for TLDs). If we cannot ensure timely removal of DS records from Trust Anchor Repositories we will explore whether the issue can be reacted to by "opting out" the entire zone via NSEC3's opt-out feature.

In just about any other scenario, we can suspend DNSSEC by instructing our name servers to ignore the "DO" bit in EDNS0 or by ceasing to refresh signatures. Still, we are at the mercy of the Trust Anchor Repositories to stop setting their relying parties' expectations that we are signed. It would be good if we only had to contact IANA.

P11. Use of the secDNS:maxSigLife element in DS creation through EPP: is it required for registration; will it be honored for expiration; etc.

When the IETF discussed this parameter the situation was that the operating registries saw this as a potential for abuse by registrants. The parameter was added as an option to appease some members of the working group whose focus was on the nature of the cryptography and not on the impact to operations.

The reason why there is a desire to limit the signature life on a DS record is to limit the duration of a replay attack on a compromised SEP (aka KSK) key. If an SEP is compromised and is recognized as compromised, an attacker with knowledge of the private key can still wreck havoc until the signature over the recorded DS RR set expires. For this reason,

there is a cryptographic reason to keep this short.

However, if the value is short, in the normal state, the registry has to regenerate the signature frequently. This could consume CPU resources within the registry. For this reason, there is back pressure to lengthen this value.

There isn't an optimal setting. This was known when RFC 4310 was in development.

Our plan for all signatures is 30 days. This is highly tunable though. If it is decided that this duration is too long, then we can shorten it. But, the shortened value is only beneficial in the anomalous case; operationally we need to observe the rate at which registrant's SEP keys are compromised.

P12. Listing DNSSEC data from Whois requests (show an example)

Neustar does not plan to change our Whois output at this time.

P13. Domain owners with keys wanting to move to a registrar that does not support 4310

A registrant will be allowed to transfer registrars even if the gaining registrar does not support DNSSEC. We will not, as is standard with transfers, modify any of the existing RRs on the domain. We believe second-level domain registrants utilizing DNSSEC will make an educated decision regarding transferring domains from one registrar to another. In the unlikely event that this issue becomes a problem or a customer support burden, we will consider alternatives, including certification and classification of registrars, and restricting transfers. At this time we do not believe this is necessary.

P14. Specifying the RFC 5155 opt-out policy

We will not use RFC 5155 in the BIZ zone unless there is some situation as described in P10 where we need to cease DNSSEC for our registrants.

We have two motivations for not deploying RFC 5155. One is that it is not required. Two is that with opt-out attackers can still cache-poison in an unsigned zone, which is one of the vulnerabilities that we want to eliminate.

P15. Salt size and hash iterations policy for RFC 5155

We plan to abstain from RFC 5155.

P16. Changing Neustar's implementation of RFC 5155 based on different resolver interactions

We plan to abstain from RFC 5155.

P17. The minimum number of registrars required to have passed OT&E before any registrar will be permitted to put DS records in the registry

There is no minimum requirement to pass an OT&E certification.

P18. The minimum number of registrars required to have passed OT&E that would cause Neustar to stop offering DNSSEC resolution

There is no minimum requirement to pass an OT&E certification.

O1. Testing to show that the DNS server components can handle the additional overhead of DNSSEC resolution

Our testing of the .BIZ zone included going from an unsigned zone to a signed zone, query performance testing with 0% of domains signed, 25% signed, 50% signed and 95% signed. We tested query and dynamic update performance.
Our testing showed increased usage in regards to system resources but we saw no visible impact on resolution performance for DNSSEC -enabled queries.

O2. Testing to show how the increased size of the zone will affect synchronization across the DNS server components

We performed tests on the BIZ zone with varying percentages of it sized while performing dynamic updates from the SRS. We saw no measurable different in the performance of dynamic update during normal operations. We did find that the use of AXFR to be inefficient in publishing the zone to throughout the constellation when first signed. We have therefore developed an out of band process to bootstrap the initial signing.

O3. Ways to report on failure modes such as clock drift on validators, DNSSEC-challenged CPE equipment, and so on

Neustar maintains active involvement in forums such as OARC, NANOG, RIPE and
IETF where operational challenges such as these are routinely discussed. Failures that are raised on those venues will be noted and evaluated.

Neustar will publish an e-mail address that can be used by end-users to report problems relating to a signed BIZ zone. Any substantial corrective action taken in response to such reports will be made public on Neustar and Neustar web pages.

O4. Interoperability testing with RFC 5155 resolvers

We abstain from RFC 5155.

O5. When the KSK compromise plan will be complete

See the earlier description of emergency key changes.

O6. Whether the ability to add DS records to the registry be disabled for registrars who have not passed OT&E

Neustar will not require registrars to certify through OT&E so they will be able to submit DS records in production once we are live with DNSSEC.

T1. List all the DNSSEC operations that are associated with a domain record

Regarding the domain update command, the following operations are supports:

o Add DNSSEC data of a domain
o Remove DNSSEC data of domain
o Modify existing DNSSEC data of a domain

Regarding the domain info command:
o List details of all DNSSEC data associated to the domain

Regarding the domain create command:
o Add DNSSEC data associated to the domain at creation

*T2. Which SHOULDs in RFC 4033, 4034, 4035, 4310, and 5155 does Neustar *not* intend to do, and why*

We are not implementing RFC 5155 because NSEC is the basic means for providing negative answers in DNSSEC. NSEC3's increment upon NSEC provides no advantages to BIZ and represents some disadvantages.

NSEC3's primary asset is prevention of discovery of the zone's contents. For BIZ, this is not a benefit as the zone file is available to all submitting to an AUP.

NSEC3 increases the size of some negative answers and requires more management of the "salt" used for NSEC3.

The NSEC3 Opt-out variant would save the generation and management of DNSSEC records, but at the risk that cache poisoning could add an unauthorized and unsigned, false delegation in the BIZ domain.

RFC 4033 has no requirements language.

RFC 4034 has only one SHOULD that appears to be compliant with BCP 14 (aka RFC 2119) and we comply with that.

RFC 4035, only sections 2 and 3.1 have SHOULDs that apply to authoritative name service. The following two SHOULDs in section 2.4 are not possible to implement:

The DS resource record establishes authentication chains between DNS zones. A DS RRset SHOULD be present at a delegation point when the child zone is signed.

The previous cannot be implemented because we do not know the status of the registrant's zones, if we did, we do not know if the zone is intended to be seen as signed. We cannot count on having a business relationship with the operator of the zone, so we cannot establish a trustworthy transport to grab the DNSKEY set and create a DS set using a hash algorithm of their choice, etc.

A DS RR SHOULD point to a DNSKEY RR that is present in the child's apex DNSKEY RRset, and the child's apex DNSKEY RRset SHOULD be signed by the corresponding private key.

The previous cannot be implemented because this is placing a requirement on an action that can only be taken by the registrant. Even if we restricted DS records to those that did refer ("point") to an entry in the DNSKEY RR set, we can't ensure that the set is signed (as we would or should not have access to the private key).

RFC 4310 has 2 problematic SHOULDs.

In section 2:

The key data SHOULD have the Secure Entry Point (SEP) bit set as described in RFC 3757 [9].

As we are accepting DS data from the registrant (via the registrar) we don't have the DNSKEY RR to inspect the SEP bit.

In section 3.1.2:

A client SHOULD specify the same <secDNS:maxSigLife> value for all <secDNS:dsData> elements associated with a domain.

This is a SHOULD on the client, not us. We can't control this action, even if we plan to reject all requests for maxSigLife

settings other than our default.

T6. There are different views about whether or not a change in the holder of a domain, the tech contact for a domain, or the registrar of a domain should cause the keys published in the zone to change; please comment on how Neustar views this

For the domain contacts, it is left up to the discretion of the registrar. It is not required to submit new DS information via EPP if any or all of the contacts change, as it is assumed that the DS information relates to the owner of the domain, not the individual contacts.

Since Neustar has no way of establishing if DS information was created by the registrant or the registrar, the registry should not enforce changing the DS information when a transfer occurs.

T7. List any DNSSEC operation that is automatically triggered by changing the registered name holder of a domain

No DNSSEC operations are automatically triggered for this case.

T8. List any DNSSEC operation that is automatically triggered by changing the technical contact of a domain

No DNSSEC operations are automatically triggered for this case.

T9. List any DNSSEC operation that is automatically triggered by changing the registrar of a domain

No DNSSEC operations are automatically triggered for this case.