ICANN Registry Request Service

Ticket ID: L0D7R-4D7P4
Registry Name: SITA
gTLD: .AERO
Status: ICANN Review
Status Date: 2010-11-24 12:07:59
Print Date: 2010-11-24 12:08:15

Proposed Service

Name of Proposed Service:

DNSSEC Implementation for .AERO

Technical description of Proposed Service:

This is a request by Societe Internationale de Telecommunications Aeronautiques (SITA) for an amendment to the .AERO registry agreement (the "Agreement").

This request is to change the function of the registry and the corresponding WHOIS and DNS systems for the .AERO gTLD to facilitate the use of DNSSEC as specified in RFCs 4033, 4034, 4035, 5910 and 5155 (NSEC3).

SITA anticipates being signed with NSEC3 using the RSA and SHA1 algorithms (specifically DNSSEC algorithm number 7, RSASHA1-NSEC3-SHA1).

SITA anticipates a backwards-compatible change to our customers' EPP client. The change will include modifications to allow manipulation of the DNSSEC DS records by the registrar. SITA expects these changes to be in compliance with RFC 5910. Some registrars may modify their own software to reflect these changes.

SITA anticipates changes to the WHOIS subsystem that will reflect some of the DNSSEC data in the registry.

SITA will make the production changes in the OT&E environment in advance of the production system changes. Registrars that wish to utilize DNSSEC will be required to complete a DNSSEC OT&E test prior to use in the production environment.

SITA does not anticipate changes to the .AERO name servers to answer queries that request DNSSEC data for validation of the response.

SITA anticipates publishing its public key information (DS records) in the root zone.

SITA anticipates no changes in rate-limiting and add storm limiting policies and practices.

SITA anticipates additional reports to be delivered to registrars that enumerate which domain names are signed, along with their expiration time stamp. Other reports may become available later. SITA anticipates no other changes to billing software and registrar invoices.

ICANN Registry Request Service

Ticket ID: L0D7R-4D7P4
Registry Name: SITA
gTLD: .AERO
Status: ICANN Review
Status Date: 2010-11-24 12:07:59
Print Date: 2010-11-24 12:08:15

SITA does not intend to charge an additional fee for this 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?:

SITA has not consulted with any community or experts.

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

SITA has not consulted with the sponsored TLD community.

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

SITA has not consulted with gTLD registrars or the registrar constituency. Because DNSSEC in .aero will comply with the Internet standards and will be offered as a voluntary, opt-in service, SITA determined that registrar consultations were unnecessary.

Once DNSSEC has been approved and implemented at the registry level, SITA 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?:

SITA did not deem consultations with any other constituency group appropriate, and has not consulted with any other constituency groups.

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

ICANN Registry Request Service

Ticket ID: L0D7R-4D7P4
Registry Name: SITA
gTLD: .AERO
Status: ICANN Review
Status Date: 2010-11-24 12:07:59
Print Date: 2010-11-24 12:08:15

SITA did not deem consultations with end users appropriate, and has not consulted with any 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 other gTLDs (.ORG, .MUSEUM, .BIZ, .CAT).

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

Because DNSSEC has been accepted as the standard for securing the DNS, SITA does not believe that there would be objection to this service.

Timeline

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

SITA plans to give immediate notification to registrars upon receipt of ICANN approval, and plans to sign the .AERO zone in the 4th quarter of 2010. Registrars will be allowed to enter DNSSEC information at a later date.

Business Description

Describe how the Proposed Service will be offered:

Adding DNSSEC security will be offered by the registrars to their customers. Once registrars have the relevant information, they will be able to manipulate the DS Resource Records in the registry using EPP (as described in RFC 5910).

Once in the registry, the appropriate records will be signed on an on-going basis. This information will then be disseminated to all .AERO name servers continuously.

The .AERO public key information (DS records) will be published in the root zone as soon as that is practical to do so. All changes in the public key information will be announced to the public on the SITA web site.

End user applications that are DNSSEC-aware will ask queries of the DNS with a flag set for a signed response. The registry name servers will then respond with the correct response, including the signatures for the requested records. It is up to the end user to validate the signatures returned.

ICANN Registry Request Service

Ticket ID: L0D7R-4D7P4
Registry Name: SITA
gTLD: .AERO
Status: ICANN Review
Status Date: 2010-11-24 12:07:59
Print Date: 2010-11-24 12:08:15

Describe quality assurance plan or testing of Proposed Service:

SITA will conduct internal testing of the .AERO 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 the SITA test environment, 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, SITA will be conducting internal testing of its registration and resolution platforms to:

- Demonstrate that all the components involved in signing .AERO domains are functioning properly;
- Document any points at which the expected behavior differs from actual behavior; and
- 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 SITA's service level agreements.

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

The relevant RFCs are: 4033, 4034, 4035, 5155 (NSEC3) and 5910.

Contractual Provisions

List the relevant contractual provisions impacted by the Proposed Service:

Section 3.1(c)(i) Data Escrow of the Registry Agreement (6 December 2006) between ICANN and SITA.

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

SITA does not expect to add any additional reports to ICANN for this service.

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

The WHOIS will now include data to show that the domain name is signed. It will not include any DNSSEC data that would

ICANN Registry Request Service

Ticket ID: L0D7R-4D7P4
Registry Name: SITA
gTLD: .AERO
Status: ICANN Review
Status Date: 2010-11-24 12:07:59
Print Date: 2010-11-24 12:08:15

compromise the security of the domain name, such as a private key.

Contract Amendments

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

Amend Section 3.1(c)(i) Data Escrow of the Registry Agreement (6 December 2006) between ICANN and SITA to read as follows:

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).

Benefits of Service

Describe the benefits of the Proposed Service:

SITA believes that the Internet user community will be better able to conduct secure transactions on the Internet with .AERO websites, because DNSEC will facilitate browsers that choose to validate that they have the correct IP address for .AERO websites.

Competition

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

SITA believes that the implementation of DNSEC in the .AERO registry system is needed to improve the security of the Internet infrastructure as a whole, will enhance the protection services 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,

ICANN Registry Request Service

Ticket ID: L0D7R-4D7P4
Registry Name: SITA
gTLD: .AERO
Status: ICANN Review
Status Date: 2010-11-24 12:07:59
Print Date: 2010-11-24 12:08:15

and give consumers more choices thereby enhancing competition.

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

This service will be available to every .AERO domain name holder.

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

There are no similar services that can provide this service for the .AERO domain.

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.:

SITA is working with its back end service provider, Afilias Limited to provide this service for the .AERO domain.

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.:

Once this application is approved, SITA will reach out to all the .AERO registrars and alert them to the introduction of this service. SITA will give registrars sufficient notice of any changes to registrar clients.

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).:

SITA does not have any such documents.

Security and Stability

ICANN Registry Request Service

Ticket ID: L0D7R-4D7P4
Registry Name: SITA
gTLD: .AERO
Status: ICANN Review
Status Date: 2010-11-24 12:07:59
Print Date: 2010-11-24 12:08:15

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

Yes. As specified by RFC 5910, registrars will have the ability to enter and manipulate DNSSEC DS records.

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

DNSSEC requires proper configuration, as well as periodic maintenance, in order to work correctly. Once properly installed and configured, the resolvers must perform the additional step of signature validation. This will cause resolution of signed Resource Records to take slightly longer. It will not impact the resolution of names that are not signed.

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

SITA is not aware that any technical concerns have been raised about the proposed service.

Other Issues

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

SITA is not aware of any.

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

No.

List Disclaimers provided to potential customers regarding the Proposed Service:

N/A

Any other relevant information to include with this request:

1. For more information on NSEC3, please see http://www.nsec3.org/

ICANN Registry Request Service

Ticket ID: L0D7R-4D7P4
Registry Name: SITA
gTLD: .AERO
Status: ICANN Review
Status Date: 2010-11-24 12:07:59
Print Date: 2010-11-24 12:08:15

2. In anticipation of possible questions from the RSTEP Review Team, consistent with the .ORG application, SITA provides the following information:

1. What plan does SITA have to recover from a .AERO KSK or ZSK private key compromise?

SITA acknowledges the importance of having a robust procedure established for reacting to a KSK or ZSK compromise.

Once the compromise plan is complete and has received satisfactory peer review, it will be made public. SITA will not publish a signed .AERO zone before a satisfactory compromise plan has been published.

Draft Compromise Plan Summary

1. Create a new public-private key pair (KSK and ZSK as needed).
2. Resign and immediately publish the .AERO zone, including revoking the compromised key.
3. If the KSK was compromised and the .AERO public key information is not in the root zone, execute an emergency update of the ICANN ITAR.
4. Execute an emergency communication plan that widely publicizes the actions of Steps 1, 2, and 3.
5. Identify the attack vector for the compromise.
6. Review the security infrastructure and mitigate the attack vector

2. The request points out that Registrars will be able to manipulate customer DS records in the registry using EPP.

Can you provide additional clarity regarding Registrar control and/or ownership of DS record information?

The Registry will treat the DS data in the same manner that other DNS and WHOIS information provided by the registrar is treated. It is the responsibility of the registrar to ensure that all data sent into the registry is factual and correct.

3. What plan does SITA have to respond to Registrar failures relating to DNSSEC issues?

In the event of a failed Registrar that runs DNSSEC, the Registry will require that the Gaining Registrar be able to run DNSSEC as well. It will be the responsibility of the Gaining Registrar to determine which DS records were generated by the Registrant, which were generated by the Losing Registrar, and which were generated by third parties. The Gaining Registrar will need to submit new DS data for those domain names signed by the Losing Registrar. The new DS data may come from the Registrant, a third party, or the Gaining Registrar as preferred by the Registrant. The Gaining Registrar should plan its

ICANN Registry Request Service

Ticket ID: L0D7R-4D7P4
Registry Name: SITA
gTLD: .AERO
Status: ICANN Review
Status Date: 2010-11-24 12:07:59
Print Date: 2010-11-24 12:08:15

interface with Registrant accordingly.

In the best interest of the Registrant community as a whole, the Registry will not delete any DS, RRSIG, or other information from the Registry or the zone. Doing so would cause inconsistencies between the Gaining Registrar's data and the Registry, as well as having the potential for a large number of validly signed zones to become unusable to DNSSEC-aware resolvers.

4. What plan, if any, does SITA have to educate the public regarding DNSSEC usage on .AERO?

The following are examples of SITA's plans to assist in the education of the public regarding DNSSEC:
- Public presentations to the technical community who run DNS resolvers, such as ISPs.
- Provide DNSSEC marketing/training materials to our registrars that they can present to their customers.
- Post DNSSEC informational materials on the public area of the SITA website.
- Provide workshops and surveys to end user community.