Name of Proposed Service: MUSEUM-DNSSEC

Technical description of Proposed Service

After a lengthy period of testing DNSSEC functionality in a sequestered namespace, the published .MUSEUM zone file was signed on 18 September 2008 at 0830 UTC. The immediate purpose of this was to confirm the positive results of the private testing, but the technical community noted almost without delay that signed records were being served in the public namespace and requests were made for the Key Signing Key and policy documentation. We therefore placed the KSK at

https://ens.museum/dnssec/Kmuseum.+005+39226.key

but made limited mention of its availability, and of the signing of the zone, pending confirmation from ICANN that the introduction of this facility was consistent with established procedure.

The present request is specifically intended to enable that determination. Its scope is restricted to the TLD zone and a limited number of as yet unsigned second level domains operated directly by the TLD sponsor for its own administrative activities; i.e. all key signing covered by this request is restricted to the agency that is responsible for the signing of the .MUSEUM zone.

We intend to develop procedures for allowing the operators of delegated second-level domains to sign their zones autonomously in the shortest time possible, but will be submitting a separate request for authorization to introduce that service. Its detail will be determined during the course of a period of consultation within the target community, which is presently largely unaware of the benefit that DNSSEC can provide. Adequate familiarization with the impending gain will require the demonstration of the signed parent zone, together with selected subdomains operated directly by the Sponsor.

Consultation

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

Initial plans for signing the .MUSEUM zone were discussed with Dr. Stephen Crocker, Chair of the Security and Stability Advisory Committee. The progress of this action has been reported to him periodically throughout the ensuing action.

The methodology and policies that we intend to apply in our broader deployment of DNSSEC are based on those developed by the operator of the .SE zone, with the smallest possible degree of adaptation. This is being done with the encouragement and consent of the .SE operator (with whom the .MUSEUM Sponsor has a long-standing collaboration in the development of IDN policy and practice). The DNSSEC policies and procedures developed for the .SE zone have been adopted with permission for the .MUSEUM zone.

The release of the signed zone on 18 September, as described above, was raised for immediate

discussion on the dnssec-deployment discussion list. The .MUSEUM implementation was received favorably, as can be seen in the list archive at http://mail.shinkuro.com:8100/Lists/dnssec-deployment/

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

No service has been offered to the sponsored community. The development of that service is contingent upon the response to the present request and will be detailed in a separate request to be submitted at an appropriate later date.

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

This was not a relevant consideration for the present action. The subsequent expansion of this service will include consultation with the .MUSEUM registrars., and be announced to other ICANN accredited registrars with particular interest in DNSSEC.

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

No such consultation was relevant to the present action, except within the security community as indicated above.

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

This action will attach to the planned extension of the service as it will be described in the subsequent request.

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

In addition to the contact described above, we acted on the further encouragement from the SSAC as indicated in http://www.icann.org/committees/security/sac026.pdf.

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

Proponents of an insecure namespace can be expected to object to this service. We assume that any such dissatisfaction would be made known via the SSAC or other relevant segments of the technical community.

Timeline

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

The signing of the TLD zone was commenced as indicated above. The subsidiary administrative zones will be signed within 30 days of the approval of this request.

Business Description

Describe how the Proposed Service will be offered

An unsigned zone file is generated from the registry database precisely as it always has been. This file has administrative zone key data inserted and is then signed externally prior to its publication. The signing of the .MUSEUM TLD zone is therefore without consequence for the registry database, and the security enhancement is entirely transparent to the registrars and registrants. (Again, it is fully recognized that this will no longer pertain when the signing of autonomous subdomains has commenced, but that phase of the action will be detailed in the separate request.)

Pending the approval of the present request, we will notify IANA that the zone is signed and request that the KSK key be included in the ITAR.

Describe quality assurance plan or testing of Proposed Service

The signed .MUSEUM zonefile is scrutinized manually before its publication. It must be noted that the state of the unsigned zone typically changes only a few times weekly and the task of ensuring the quality of its signed correlate is of a significantly smaller scale than is the case with any of the other signed TLDs.

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

The normative and narrative instruments that generally attach to DNSSEC are also relevant to the present action. These currently include RFC 4033 (DNS Security Introduction and Requirements), RFC 4034 (Resource Records for the DNS Security Extensions), and RFC 4035 (Protocol Modifications for the DNS Security Extensions) and will be augmented by NSEC3 as described in RFC 5155 (DNS Security (DNSSEC) Hashed Authenticated Denial of Existence). In addition, the procedural specifications for the .SE implementation of DNSSEC are being adapted for .MUSEUM.

Contractual Provisions

List the relevant contractual provisions impacted by the Proposed Service

The proposed service has no contractual impact, although a subsequent request to make DNSSEC available in subzones will require a change to the Data Escrow provisions in Section 3.1(c)(i) of the .MUSEUM TLD Sponsorship Agreement.

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

None, but note that DS records for the administrative subzones described earlier would become part of any escrow provisions for registry continuity.

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

None.

What effect, if any, will the proposed service have on the price of a domain name registration?

None.

Contract Amendments

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

The present action does not require contractual amendment.

Service Benefits

Describe the benefits of the Proposed Service

The benefits of the proposed service are those that are generally expected to derive from the DNSSEC signing of TLD zones. These are focused on reducing the vulnerability of the DNS to ill-intended exploitation, for example, through the protocol flaw recently described by Dan Kaminsky. The signing of a gTLD zone is also expected to provide further impetus toward the signing of the root zone, as well as encouraging the signing of other gTLDs -- an aggregate action that is ultimately necessary if the DNS is to be secured from disruption of the type just referenced.

Competition

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

The proposed service is without competitive effect.

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

It is not a competitive service.

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

The only comparable facility would be another signed TLD.

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?

We do not expect the signing of the .MUSEUM TLD in any way to impair the competitive ability of any other entity.

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.

The .MUSEUM sponsor has always been directly responsible for the publication of the .MUSEUM zone file, which is generated automatically from the registry database at regular intervals. The signing of the zone file is an intermediate step between these actions and is also conducted by the sponsor.

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. 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).

These considerations are not relevant to the present action.

Security and Stability

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

The proposed service is conducted entirely externally to the registry and does not alter the registry data in any way. It should be noted, however, that the DS records for the administrative sub-zones described above will become part of the escrow provisions for registry failover.

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

The review of the signed zone file may delay its publication, but the interval is without consequence for Internet servers and end systems.

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

No such concerns have been raised.

Other Issues

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

No.

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

No.

List Disclaimers provided to potential customers regarding the Proposed Service

None are deemed necessary at this juncture.

Any other relevant information to include with this request