ICANN Registry Request Service

Ticket ID: Q3D5W-0G6V2
Registry Name: Fundació puntCAT
gTLD: .CAT
Status: ICANN Review
Status Date: 2010-02-23 09:00:11
Print Date: 2010-02-23 09:00:19

Appendix {A(CATfReqDNSSEC(2).pdf)
(Seen on Next Page)

core Internet Council of Registrars

ICANN Registry Request Service

DNSSEC for .CAT

Version 1.0

CORE Internet Council of Registrars

2010-02-17

Table of Contents

1. ICANN Registry Request Service

1.1 DNSSEC Introduction

1.1.1 Terminology

A "resolver" is something that implements the "resolver" (ie, client) role in the DNS protocol. It might be a stub resolver, the client side of a recursive name server, or a pure iterative resolver, ... The defining characteristic is that it sends queries (QR=0) and receives responses (QR=1).

A "name server" is something that implements the "name server" (ie, server) role in the DNS protocol. It might be an authoritative name server, the server side of a recursive name server, ... The defining characteristic is that it receives queries (QR=0) and sends responses (QR=1).

In the discussion which follows, we use "resolver" and "name server" in this sense.

1.1.2 Technical Description

The DNS Security Extension Protocol (DNSSEC) is a collection of new resource records and protocol modifications that adds data origin authentication and data integrity to the DNS. The design goal of DNSSEC, originally funded by the United States Defense Advanced Research Projects Agency (DARPA), is to allow resolvers to detect responses which contain forged data, e.g., through cache poisoning. All QR=1 responses by DNSSEC enabled name servers are digitally signed, and by checking the digital signature, the query issuing QR=0 resolver is able to determine if the response is identical to the response the resolver would have gotten had it directly queried the authoritative name server.

These mechanisms require changes to the DNS protocol. DNSSEC adds four new resource record types: Resource Record Signature (RRSIG), DNS Public Key (DNSKEY), Delegation Signer (DS), and Next Secure (NSEC). These new RRs are described in detail in RFC 4034.

It also adds two new DNS header flags: Checking Disabled (CD) and Authenticated Data (AD). In order to support the larger DNS message sizes that result from adding the DNSSEC RRs, DNSSEC also requires EDNS0 support (RFC 2671).

Finally, DNSSEC requires support for the DNSSEC OK (DO) EDNS header bit (RFC 3225) so that a security-aware resolver can indicate in its queries that it wishes to receive DNSSEC RRs in response messages. By checking the signature, a DNS resolver is able to check if the information is identical (correct and complete) to the information on the authoritative DNS server.

The implementation of this collection of resource records and protocol modifications is commonly referred to as *signing the zone.* The .cat zone will be signed by the puntCAT registry.

The puntCAT registry will implement the modifications to the Extensible Provisioning Protocol (EPP) defined in RFC 4310 which allow registrars to submit

DS record data as part of the provisioning payload in XML format. This will allow .cat registrars to provision signed data for registrant domains, extending the data origin authentication and data integrity property from the .cat zone itself to any sub-zone (domain) for which the registrant seeks, and the registrar offers, to sign the domain data.

1.1.3 Threat Environment

DNSSEC services protect against most of the threats to the Domain Name System. There are several distinct classes of threats to the Domain Name System, most of which are DNS-related instances of more general problems, but a few of which are specific to peculiarities of the DNS protocol.

Note that data origin authentication and data integrity provide end-to-end authenticity and integrity to the query-response semantics of the DNS. These do not provide encryption (confidentiality of data) of the query payload or the response payload, or authenticate any other property of either the query issuing resolver or the query responding name server. Also, DNSSEC does not protect against DDoS attacks.

At the Summer 2008 IETF meeting in Dublin (IETF-72), the cache poisoning attack was demonstrated. At the time, it was believed that a cache poisoning attack was possible but infeasible. The demonstration consisted of two laptops, one running a recursive server, one running the cache poisoning attack. There was no external connectivity hence no risk of spread, and to make it simple, the server listened on only one port. The time from start to finish was three seconds while using non-optimized code (loops not unrolled, interpreted code, etc.). Speeding it up by a factor of three would be trivial.

This is the current threat environment: it is possible to poison any cache and offer forged data to any resolver in 60 seconds or less.

1.2 Technical description of Proposed Service

The technical description of the proposed signing and publication service is contained in the DNSSEC series of RFCs, specifically:

- RFC 4033 DNS Security Introduction and Requirements
- RFC 4034 Resource Records for the DNS Security Extensions
- RFC 4035 Protocol Modifications for the DNS Security Extensions

Additionally, the technical description of the proposed provisioning service is contained in an RFC which extends the the EPP series of RFCs:

- RFC 4310 Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)

Additionally, the technical description of the prevention of zone enumeration (zone walking) is in the following RFC:

- RFC 5155 DNS Security (DNSSEC) Hashed Authenticated Denial of Existence

1.3 Consultation

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

CORE technical staff has regularly engaged with the technical community on a broad spectrum of DNSSEC issues and has worked with organizations and individuals considered to be experts in the field of DNS. A partial list of CORE's consultative engagement is:

- IANA's DNSSEC
- ISC's Initial DNSSEC Workshop;
- NIST;
- DNS-OARC (Operations, Analysis, and Research Center);
- IETF DNSEXT Working Group;
- IETF DNSOPS Working Group;
- NANOG;
- RIPE;
- The .SE operator;

And of course

- MuseDoma, which with CORE, signed the .museum zone at 0830 UTC, 18 September, 2008.

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

PuntCAT initiated the request for DNSSEC in 3Q09.

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

CORE is aware of course, as a registrar, that its members, and its peers in the gTLD registrar community, are not yet prepared to make use of DNSSEC.

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

CORE consulted informally with the Registry Constituency, through which it participates as an *observer.* Additionally, CORE has consulted with the GNSO's Security and Stability related activities, e.g., the FastFlux PDP WG, members of the SSAC, and members of the RSAC.

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

CORE consulted informally with browser vendors, public administrations and banking and finance groups.

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

The introduction of DNSSEC is endorsed by the US Department of Commerce (October 2008 Notice of Inquiry), the US CERT (advisory VU-800113), and ICANN's Security and Stability Advisory Committee (SSAC).

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

There are vendors of *middleware boxes* which will fail to correctly process query responses which are larger than 512 bytes, and for whom the decade old threat model (DDoS, malware, viruses, etc.) is more significant than man-in-the-middle attacks on the DNS. Additionally, consumer broadband router vendors are not yet prepared to support DNSSEC. These vendors will object to the introduction of DNSSEC.

1.4 Timeline

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

PuntCAT plans to give immediate notification to registrars upon receipt of ICANN acknowledgement and will sign the .cat zone in the first quarter of 2010. Registrars will be able to submit signed data (delegation signer (DS) resource records) via EPP, as modified by RFC 4310 Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP), directly thereafter.

1.5 Business Description

Describe how the Proposed Service will be offered:

CORE will make DNSSEC available to all ICANN-accredited PuntCAT registrars as an opt-in, value-added service. Registrars will be encouraged, but not required, to offer DNSSEC functionality to both the new and existing .cat domain names they manage on behalf of registrants.

Signing and Key Rollover

CORE will generate and hold all keys (both Key Signing Key (KSK) and Zone Signing Key (ZSK) for the .cat zone. CORE is evaluating using a hardware signing application certified at FIPS 140-2 as an alternative to manual key management.

The .cat zone will be signed with NSEC3 using the SHA-1 algorithm (specifically DNSSEC algorithm number 7, RSA-NSEC3-SHA1).

Delegation Signer (DS) and NSEC3 resource record sets (RRSets) will use a signature duration of 14 days (14d). DS RRSets will have a time to live (TTL) value of 12 hours (12h) and NSEC3 RRSets will have a TTL of 12 hours (12h). While these values specify the initial configuration parameters, CORE 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 lifetime of the KSK will be one year (1y), with manual rollover until procedures with DS records in the root zone are clear. After the first year, CORE will annually assess the viability of the key based on current cryptoanalysis techniques and only roll the KSK when it becomes necessary.

ZSK - The ZSK will be a 1024 bit key. The lifetime of the ZSK will be 30 days (30d), with pre-published rollover.

Describe quality assurance plan or testing of Proposed Service:

CORE will conduct internal testing of the puntCAT registry to verify functionality and performance with DNSSEC-enabled domain names.

The primary goal of the testing is to exercise the registration and resolution systems in CORE's test environment by managing the DS record provisioning for test names and querying DNS for the registered test names.

Specifically CORE will conduct internal testing of its registration and resolution platforms to:

- demonstrate that all components involved in signing .cat are functioning properly;
- document any points of departure between expected and observed behavior; and
- measure throughput and performance of the provisioning platform, updates to the name server constellation and resolution of the names in the test environment

to verify that DNSSEC may be introduced without impact to CORE's and PuntCAT's service level agreements. This end-to-end testing will ensure that all involved systems are functioning correctly, including:

- registrar provisioning of the registry via EPP modified per RFC 4310;
- zone file publication updates; and
- DNS resolution in the test environment.

While CORE does not register .cat names as a matter of policy, to avoid conflict of interest, CORE's registrar function will additionally test CORE's registry, similar to Verisign's use of the EDUCAUSE registrar, the sole registrar for the Verisign operated .edu registry, to conduct end-to-end testing of DNSSEC-enabled names in a non-production environment. The test results obtained through collaborative testing will provide CORE and PuntCAT with information and data on the code base and business processes that PuntCAT intends to use with its production registrars.

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

- RFC 4033 DNS Security Introduction and Requirements
- RFC 4034 Resource Records for the DNS Security Extensions
- RFC 4035 Protocol Modifications for the DNS Security Extensions
- RFC 4310 Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)
- RFC 5155 DNS Security (DNSSEC) Hashed Authenticated Denial of Existence

The first three define DNSSEC, the fourth defines how DS data is provisioned via EPP, and the fifth defines how zone enumeration (zone walking) may be prevented.

In addition, the procedural specifications for the .se implementation of DNSSEC are adapted for .cat.

Further, the ongoing development of key timing considerations in

- draft-morris-dnsop-dnssec-key-timing-xx.txt.

1.6 Contractual Provisions

List the relevant contractual provisions impacted by the Proposed Service:

No contractual provisions will be impacted.

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. In the future, there may be some utility for including DNSSEC data in WHOIS output.

1.7 Contract Amendments

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

No contractual amendments are required.

1.8 Benefits of Service

Describe the benefits of the Proposed Service:

While significant threat other than that posed by Man-in-the-Middle (MitM) attacks exist, see RFC 3833 Threat Analysis of the Domain Name System (DNS), the triviality of cache poison attacks targeting specific caches and specific RRSets makes the adoption of DNSSEC mandatory to implement for registrants seeking fundamental proof of correctness to resolvants (persons and applications attempting to correctly resolve the resource associated with the registered domain name).

CORE believes that the introduction of DNSSEC functionality in the .cat registry and resolution system will benefit the Catalan Internet community by improving the security of the .cat name space and decrease the likelihood that Catalan, and non-Catalan registrants, and users, will be subject to MitM and cache poisoning attacks.

1.9 Competition

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

CORE believes that the implementation of DNSSEC into the puntCAT registry system 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 Catalans more choices thereby enhancing competition.

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

The low cost of implementing cache poison implies that the market for DNSSEC are those registrants which solicit any form of e-commerce, including charities, where the cash value of a single transaction is measured in modest dollar (euro) amounts. Additionally, registrants which have an informational or reputation value are part of the DNSSEC market. Furthermore, registrants which wish to provide additional layers of trust to their customers are a market for DNSSEC service.

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

The following gTLDs are currently signed and will be offering second level DNSSEC domain signatures:

- .museum
- .gov
- .org

The following country code TLDs operate a signed zone:

- Brazil (.br)
- Bulgaria (.bg)
- Czech Republic (.cz)
- Puerto Rico (.pr)
- 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, signing the .cat zone can only be offered by the puntCAT 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.:

The backend service provider for .cat is CORE.

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.:

As in Consultation (f), there are vendors of *middleware boxes* which will fail to correctly process query responses which are larger than 512 bytes. This problem is not particular to the puntCAT registry or to the Catalan users, but generic, and the vendors are aware of their technical problems.

In addition to the communication and survey with the puntCAT registrars, PuntCAT and CORE are pursuing an interoperability lab for vendors present in the Franco-Iberian market to review their equipment and services 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).:

PuntCAT and CORE have no additional documents to submit.

1.10 Security and Stability

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

DS records are provisioned and stored.

The implementation of DNSSEC will allow registrars to submit DS record data to the Shared Registry System as recommended in RFC 4310. CORE's registry system will allow addition or deletion of DS records related to a .cat 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 responses to Internet servers or end systems:

Nominal change due to increased record size. Signed DNS records are significantly larger than the records of current, unsigned domain names. This accounts for the failure at 512 bytes manifested by *middlebox* vendor, noted elsewhere. 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, CORE has upgraded its system, currently tested to 25,000,000 domains, and CORE does not anticipate the additional size and processes to exceed the service level agreements in the current registry agreement.

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

Yes. There is a significant level of concern in the operations community due to the operational novelty of DNSSEC. This concern is characterized by:

- understanding and complexity with signing domain names and managing keys and key rollovers;
- the ability for current, and older network equipment to receive and process the larger DNSSEC enabled queries and responses -- the 512 byte problem mentioned earlier.

CORE and PuntCAT will provide the puntCAT registrar community with educational materials and an implementation guide to sign and manage DNSSEC enabled domains.

1.11 Other Issues

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

CORE and PuntCAT are not aware of any intellectual property considerations.

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

No.

List Disclaimers provided to potential customers regarding the Proposed Service:

CORE and PuntCAT will provide industry standard disclaimers, such as disclaimer of all warranties, in the service agreement.

Any other relevant information to include with this request:

None.