Puerto Rico Top Level Domain — dnssec

Dr. Oscar Moreno, Manager and Founder, moreno@nic.pr
David Soltero-Lugo, david@nic.pr
Pedro Campos, pedro@nic.pr

Why was NIC.PR interested in Implementing DNSSEC?

NIC.PR is a Research Laboratory involved in various research projects that include:

- – Watermarking
- – Public Key Cryptography

Currently edit journal
- – Design, Code and Cryptography

Being a technology center of Computing Science NIC.PR considered DNSSEC to be an area of interest.

What is DNSSEC

DNSSEC is "DNS Security Extensions"

How it works:

- DNS Data authenticity and integrity by:
  - Generating a public/private key set
  - Signing the Resource Records Sets with the private key.
  - The public key is used to verify the Resource Records signatures
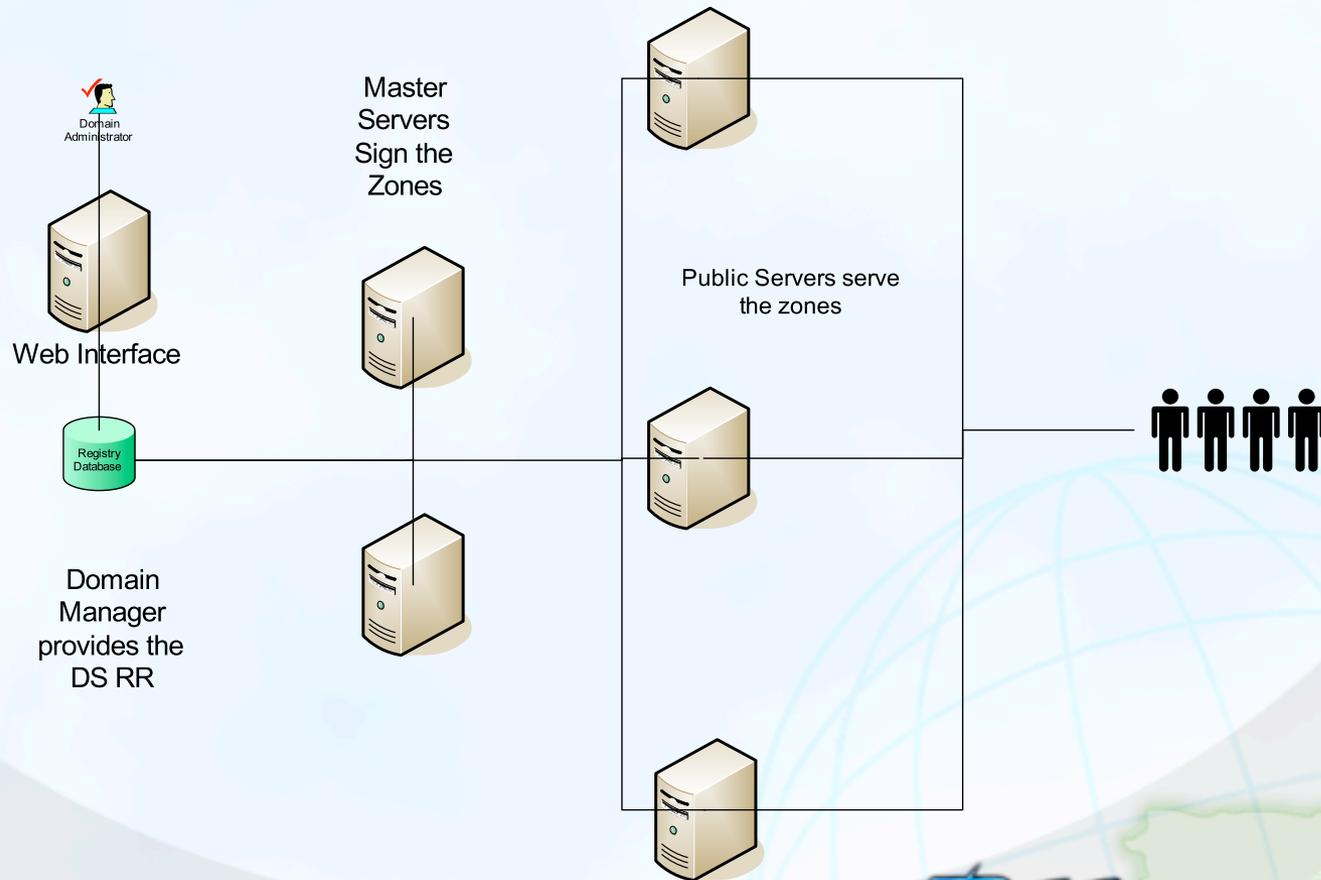 - Authenticity of the key is established by the DNSKEY checksum at the parent zone (DS RR)

When was DNSSEC Activated?

- NIC.pr started signing the zones on JULY 2006

- NIC.pr started transmitting DNSSEC zones to the public server for the first time in August 2006.

- Currently 19 zones are currently signed. (.pr + 18 2nd Level)

pr PUERTO RICO
Top Level Domain

Why was NIC.PR interested in Implementing DNSSEC? cont..

- – (2000) The Local Government Site was redirected to a Pornographic Site at the ISP Level
    - Had DNSSEC technologies been available at the this could have been avoided.
- – We believe in DNSSEC as the way to go to implement DNS Security.

How it works

Domain
Administrator

Web Interface

Registry
Database

Domain
Manager
provides the
DS RR

Master
Servers
Sign the
Zones

Public Servers serve
the zones

pr PUERTO RICO
Top Level Domain

Why now and Not Later ?

- Thru out the years cryptography schemes, have evolve as needed, to keep up modern security capabilities in order to keep up with threats. (like the SSL with 64Bit Cryptography, know at 128Bits+)
  - We believe that is the case of DNSSEC.
- We believe that "The problem is worst than the solution"

PUERTO RICO
Top Level Domain

DNSSEC Vulnerability

- Currently a disadvantage of using DNSSEC is the threat of DNS WALKS
  - By walking the zone, a list of all the records can be obtain
    - This is pending a solution, but there are other possible solutions:
      - RFC 4470 – Minimally Covering NSEC Records and DNSSEC On-line Signing. Some safety considerations for RFC 4470 are:
        - Private key most reside at the public servers
        - On demand zone signing is computationally intensive (DoS)
        - Unknown epsilon function predictability

What NIC.pr has done with DNSSEC.

- Empowered Registrars to use and administer there own keys in and automated fashion and to create trusted relationship between Parent and Child Zones.
  - Thru a registration interface.

- Provide a Portal in order to educated Registrars end-users on how to use and authenticate with DNSSEC.

Advantages of programmed Interface

Registers

- Keys can be set at any moment and updated at will and immediately without NIC.PR administrator interaction. Multiple keys are supported, providing room multiple DS records.

- Validates the domain user will establishing a trusted link between Parent Zone and Child Zone

End Users

- DNSSEC application can authenticate Zones without having to manually retrieve the Child Zone Key manually making the authentication easier.

How Trusts between Parent and Childs are Setup

- Child Domain Management Interface provides ability for Registrar delegate DNSSEC to PR

| Edit | Renew Domain | Register Domain | User Information | Whois Configuration | Search | Check Out |

Domain Name	Type			
nic	pr	Contact Information	Change Nameservers	DNSSEC Record
icannsanjuan	pr	Contact Information	Change Nameservers	DNSSEC Record
	pr	Contact Information	Change Nameservers	DNSSEC Record

How Trusts between Parent and Childs Setup

- The Child Zone needs only to provide the information from the generated DS record (example:like "nic.pr. IN DS 2684 5 1 F461055CF27925A56BF9CFF1826E946235BE2767", and insert everything after word DS, Into the provided interface:

Example: your_domain_name.pr. IN DS 2684 5 1 F461055CF27925A56BF9CFF1826E946235BE2767

nic.pr. IN DS [   ] [   ] [   ] [   ]
nic.pr. IN DS [   ] [   ] [   ] [   ]

[Submit] [Return to Main Menu]

DNSSEC Resource Portal

- A Portal that will promote the use of DNSSEC, will provide resources such as:

  - Howto's
  - Download
  - Documentation
  - And related information for deployment of DNSSEC

See http://dnssec.nic.pr

What is store for the future ?

- NIC.pr is currently developing tools for the following:

    – Web based DNS authentication tool
    – Automated Key Rotations
    – Key-Signing-Key (KSK) Support
    – Dynamic tutorial of deploying DNSSEC

Thank You!
Questions ?