



.pr DNSSEC Adoption



Table of Contents

- ❖ Objectives
- ❖ Background
- ❖ Case studies
- ❖ First efforts
- ❖ Second efforts
- ❖ DNSSEC status update
- ❖ Future plans
- ❖ Conclusion

Objectives

- Promote the widespread adoption of DNSSEC in the .pr ccTLD.
- Evaluate current implementation obstacles that are preventing adoption.
- Propose solutions to aid in the process of DNSSEC adoption.

Background

- NIC.PR started signing the zones on July 2006.
- Second ccTLD to adopt DNSSEC after Sweden (.se).
First in the Western Hemisphere.
- 2010-09-23: Uploaded DS record to the root.

What we did

- Before the root zone was signed on July 2010, DNSSEC Lookaside Validation (DLV) was used to enter the Chain of Trust.
- DLV allowed validating resolvers to validate DNSSEC-signed data from zones whose parent zones either weren't signed or didn't publish DS records for their children zones.
- The Drill Extension for Mozilla Firefox was used for validation.

First Adoption Efforts

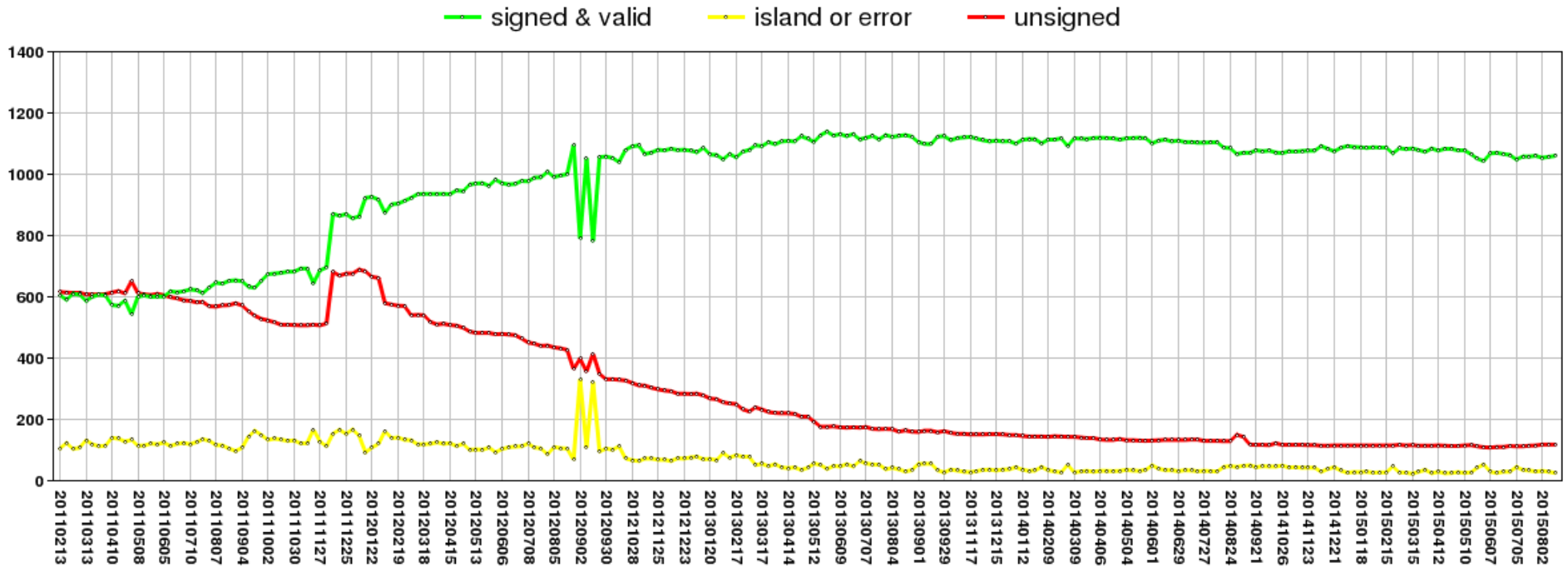
- A number of attempts urging the local community to implement the protocol were met with resistance, circa 2006.
- This inertia was due in part to:
 - Lack of technical knowledge
 - Early adoption concerns

Case studies

- .br ccTLD
 - Provides DNSSEC hosting for limited zone sizes.
 - 22% of total .br domains signed.
- U.S. Federal government
 - On 2008 the U.S. Federal government received the mandate to deploy DNSSEC to the .gov TLD.
 - 87% of .gov sub-domains signed to date.

.gov DNSSEC Adoption Timeline

USG DNSSEC Enabled Domains Over Time



Second Efforts

- Mail blast sent to selected domains (e.g., municipalities, media).
- Out of those who showed interest, none converted to a successful implementation.

Industry DNSSEC Adoption Timeline

Industry DNSSEC Enabled Domains Over Time

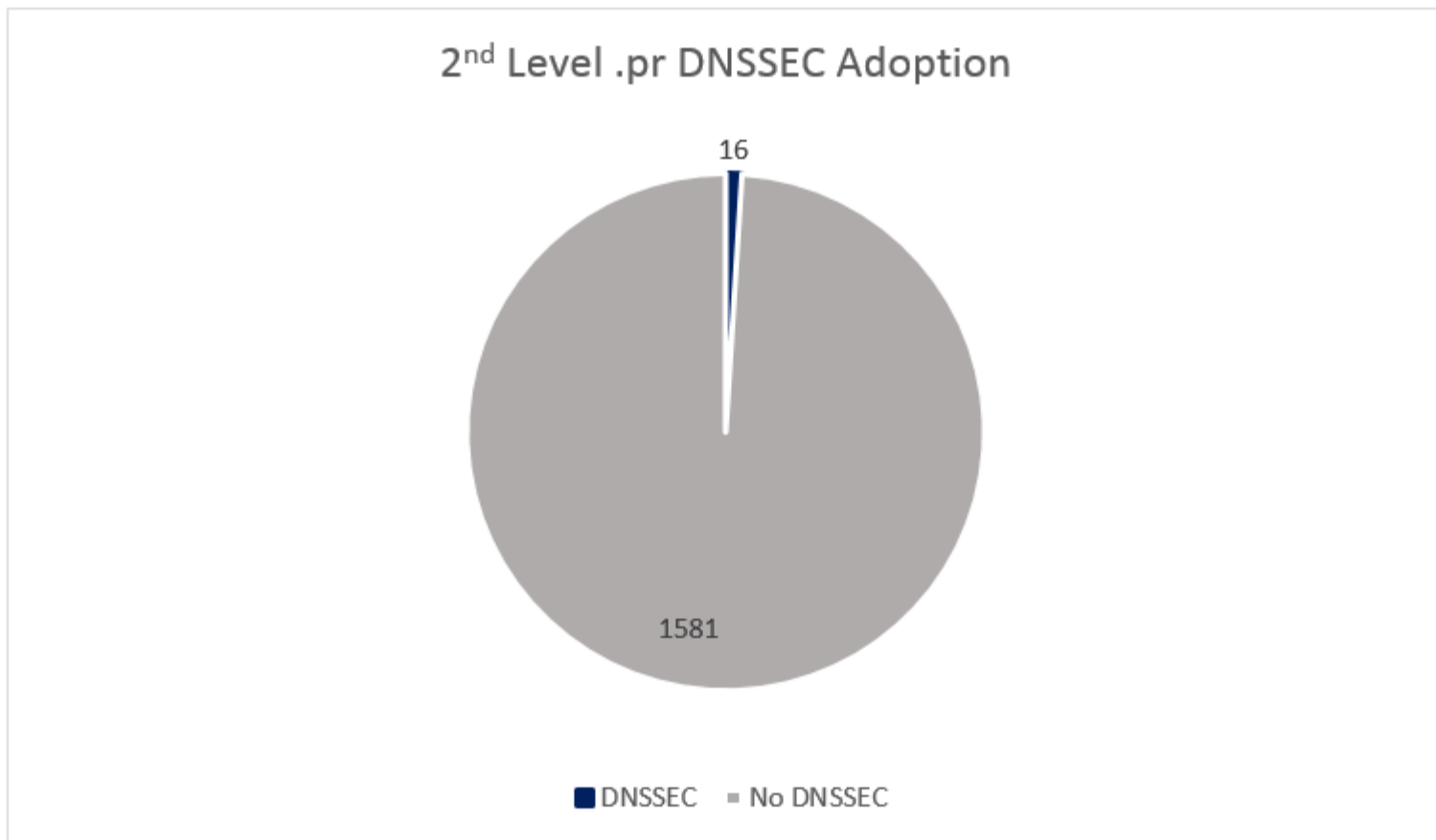
signed & valid island or error unsigned



What we are doing now

- Actively promoting the adoption of DNSSEC to our users by providing direct assistance and/or tutorials on configuration.
- For selected registered domains with incentives and for government organizations, we are hosting their zone files and enabling/managing DNSSEC for them.

2nd Level DNSSEC Adoption



Future Plans

- As a parallel approach, we are considering the initiative to offer the .com.pr extension at a 90% discount to local entities with the condition that we host and sign their DNSSEC zones.



Summary of findings

Enforcement



Good reception

Left alone



Poor reception


Economic incentive



Time will tell

Conclusion

- Clients don't mind DNSSEC as a requisite as long as they don't have to manage it (network admins included).
- People show interest and understand the benefits of the protocol.
- Implementation at the TLD level is not enough. Alternative methods need to be considered to promote the use of DNSSEC.



Thank you!
Questions?



References

Evans, Karen. "Securing the Federal Government's Domain Name System Infrastructure." Memorandum for Chief Information Officers. Executive Office Of The President. Washington, D.C. 22 Aug. 2008. Web. <<http://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2008/m08-23.pdf>>.

Khul, Rubens. ".BR DNSSEC Update." DNSSEC Workshop. ICANN 53. Web. 24 Jun. 2015. <<https://buenosaires53.icann.org/en/schedule/wed-dnssec/presentation-dnssec-br-24jun15-en.pdf>>.

"Status Update, 2010-05-05." Root DNSSEC. ICANN and VeriSign, 5 May 2010. Web. 2 Aug. 2015. <<http://www.root-dnssec.org/index.html?p=259.html>>.

"Estimating IPv6 & DNSSEC Deployment Status." Information Technology Laboratory, Advanced Network Technologies Division. NIST. Web. 2 Aug. 2015. <<http://fedv6-deployment.antd.nist.gov/cgi-bin/generate-gov>>.

"Estimating IPv6 & DNSSEC Deployment Status." Information Technology Laboratory, Advanced Network Technologies Division. NIST. Web. 8 Aug. 2015. <<http://fedv6-deployment.antd.nist.gov/cgi-bin/generate-com>>.

<http://www.suitecfo.com/images/site/strategy-banner.png>