Challenges of Deploying DNSSEC:
Prepare your ccTLD with Secondary DNS services

ICANN Brussels
June 2010

Presented by:
Roland LaPlante
SVP, Chief Marketing Officer
Afilias
Afilias Registry Services

• Afilias supports 15 TLDs today, with over 16M registrations
• IDNs and iTLDs: Afilias also supports IDN TLDs
Agenda

• DNSSEC is coming!
• DNSSEC is BIG!
• How to protect your TLD
DNSSEC is at the tipping point

Barriers

- Complexity
- Costs

Incentives

- Signed Root
- Signed TLDs: .org, .gov, .se
- Testbed deployments
- New hw & sw solutions

NO

YES

Speaker: Roland LaPlante
DNSSEC is coming

- Several TLDs have signed their zones already
  - .ORG, .GOV, .SE, .PM, BR, BG, CZ, PR (.com plans early 2011)
- Plans in place for domains to be signed as well
- The root to be signed in July, 2010
  - May 5: DURZ deployed to all 13 root servers (deliberately unvalidatable root zone) for observation
  - July: Distribution of validatable, production, signed root zone; publication of root zone trust anchor
- .ORG deploying DNSSEC for second level domains in June, 2010
- All ICANN new TLDs will be required to have DNSSEC at launch
- Afilias: supports .ORG’s deployment; provides secondary DNSSEC ready DNS service for .SE
1. DNS loads WILL increase for 3 reasons:

   • Larger Zone File Size
   
   • Greater Bandwidth Requirements
   
   • More Traffic
1. For EVERY signed domain, your zone file will now have to store and provide:
   • Digital signer record to point to the Public Key
   • Signature records

2. On average, you should expect your zone file to increase 4-6 times its current size.
   • More data = more space
1. DNSSEC responses contain more information
   • Initial DNS response (e.g.: for SOA record), PLUS
   • RRSig (Resource Record set)
   • DNSKey
2. A DNSSEC response is about 8x as big as a regular DNS query (4 kb vs. .5 kb)
3. Factor in more bandwidth and processing power to handle larger responses for EACH DNSSEC QUERY
4. Extra Bandwidth requirement: 2-4x (estimated)
• **More TCP queries:** DNS uses UDP, a lightweight protocol, to return responses for DNS queries.
  - BIND 9.4.x (and earlier versions) limit UDP responses to 512 bytes
  - Since DNSSEC information is larger (~4k), responses can be truncated
  - Those who use UDP may resend a TCP query to get DNSSEC info

  **Most signed TLDs report up to a 1-2% TCP traffic increase.**

• **Key Rollover:** No industry standards for key storage down the “chain of trust” (until root validates)
  - If a validating resolver caches an out of date key, you could see query traffic increase for those that need to renew the key

• **Traffic impact:** +1% in TCP traffic?
  - Hard to estimate until the root is signed
50% of the traffic Afilias sees TODAY asks for DNSSEC information

- The most ubiquitous DNS software – BIND – already asks for DNSSEC information built in
- This means you will be serving signature information as soon as you sign

How will you be ready for the increases in load?

Speaker: Roland LaPlante
1. Reduces the risk of load increases from DNSSEC deployment
   - Effortlessly handle significant increases in DNS load once you sign your TLD with DNSSEC.
   - Economical and risk-free way of ensuring 100% DNS up-time when deploying DNSSEC.

2. Guarantees 100% uptime of your DNS (regardless of DNSSEC)
   - Insurance against unexpected traffic spikes.
   - Protection in case of a full network outage by DDoS.
   - Protection from zero day vulnerabilities.

3. Augment your existing DNS network
   - Minimizes the expenses and capital requirements to expand your existing DNS network.
Afilias offers secondary DNS

• Secondary DNS services
• Primary DNS services
• Complete Registry + DNS services (+ iTLDs)

Special Offer:
FREE 45 days of Secondary DNS Support for ccTLDs that sign their zone with DNSSEC

Speaker: Roland LaPlante
Thank you!

Roland LaPlante

rlaplante@afilias.info

www.afilias.info/dns