This design is the result of a cooperation between ICANN & VeriSign with support from the U.S. DoC NTIA
Quick Recap

- 2048-bit RSA KSK, 1024-bit RSA ZSK
- Signatures with RSA/SHA-256
- Split ZSK/KSK operations
- Incremental deployment
- Deliberately Unvalidatable Root Zone (DURZ)
DURZ Deployment

• The Deliberately Unvalidatable Root Zone (DURZ) deployment started on January 27.

• As of today, 12 root server letters are serving the DURZ.

• J-Root begins serving the DURZ this Wednesday, May 5.

• After that, all root servers will have the DURZ.
Net Buzz

GlenQuagmire
Giggidy Giggidy
Giggidy Goo
Premium
join: 2004-02-16
Grand Rapids, MI

DNS FAIL
I break the DNS all of the time, one little mistake and no Internets (f$##ng MX records). They are so going to break the root servers.
--
Yes, its stuck in a windows this time.

permalink · 2010-04-30 09:50:01 · reply

http://www.dslreports.com/shownews/A again-DNSSEC-Updates-Shouldnt-Impact-You-108170
DNSSEC

Look...I happen to know one of the guys that is working on this very project through ICANN and I can assure you that it's in very good hands.

There is really nothing to be worried about.
## DURZ Data Collections

<table>
<thead>
<tr>
<th>Pre-DURZ</th>
<th>2010-01-19  ✔</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>2010-01-27   ✔</td>
</tr>
<tr>
<td>A</td>
<td>2010-02-10   ✔</td>
</tr>
<tr>
<td>I, M</td>
<td>2010-03-03   ✔</td>
</tr>
<tr>
<td>D, E, K</td>
<td>2010-03-24   ✔</td>
</tr>
<tr>
<td>B, C, F, G, H</td>
<td>2010-04-14   ✔</td>
</tr>
<tr>
<td></td>
<td>2010-05-05   ✔</td>
</tr>
</tbody>
</table>
UDP Query Rate

Queries Per Second

Pre DURZ 2010–01–19
L DURZ 2010–01–27
A DURZ 2010–02–10
I,M DURZ 2010–03–03
D,E,K DURZ 2010–03–24
TCP Query Rate

Queries Per Second

<table>
<thead>
<tr>
<th>Time</th>
<th>Queries Per Second</th>
</tr>
</thead>
<tbody>
<tr>
<td>16:50</td>
<td>0</td>
</tr>
<tr>
<td>17:00</td>
<td>0</td>
</tr>
<tr>
<td>17:10</td>
<td>0</td>
</tr>
<tr>
<td>17:20</td>
<td>0</td>
</tr>
<tr>
<td>17:30</td>
<td>0</td>
</tr>
<tr>
<td>17:40</td>
<td>0</td>
</tr>
<tr>
<td>17:50</td>
<td>0</td>
</tr>
</tbody>
</table>

G
UDP Priming Query Rate for the previous month as of 2010–05–01 00:00:00

A single Cisco CNR instance with max-cache-ttl=0
DS Change Requests

• Approach likely to be based on existing methods for TLD managers to request changes in root zone.

• Anticipate being able to accept DS requests in late May or early June.
Policy Update

- Updated versions of the draft KSK and ZSK DNSSEC Practice Statements (DPS) will be published shortly.
  - Not much has changed substantively, but please read these practice statements – answers to most questions regarding DNSSEC for the Root Zone can be found in the DPS.
Documentation
Available at www.root-dnssec.org

- Requirements
- High Level Technical Architecture
- DNSSEC Practice Statements (DPS)
- Trust Anchor Publication
- Deployment Plan
- KSK Ceremonies Guide
- TCR Proposal
- Resolver Testing with a DURZ
Questions & Answers
rootsign@icann.org
Root DNSSEC Design Team

Joe Abley
Mehmet Akcin
David Blacka
David Conrad
Richard Lamb
Matt Larson
Fredrik Ljunggren
Dave Knight
Tomofumi Okubo
Jakob Schlyter
Duane Wessels