DNSSEC for the Root Zone

Questions & Answers Session at IETF’77 Anaheim, March 2010

Jakob Schlyter

Richard Lamb, ICANN       Matt Larson, VeriSign
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)
What’s happened since IETF’76?
DURZ Deployment

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

• As of today – 4 root server operators are serving the DURZ.
# Root Server Status

<table>
<thead>
<tr>
<th>Root Server</th>
<th>Operated by</th>
<th>Signed ARPA</th>
<th>DURZ</th>
<th>LTQC</th>
<th>DITL</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>VeriSign</td>
<td>2010-03-16</td>
<td>2010-02-10</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>B</td>
<td>ISI</td>
<td>2010-03-16</td>
<td>2010-04-14</td>
<td>unknown</td>
<td>unknown</td>
</tr>
<tr>
<td>C</td>
<td>Cogent</td>
<td>2010-03-16</td>
<td>2010-04-14</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>D</td>
<td>UMD</td>
<td>2010-03-16</td>
<td>2010-03-24</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>E</td>
<td>NASA</td>
<td>2010-03-16</td>
<td>2010-03-24</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>F</td>
<td>ISC</td>
<td>2010-03-17</td>
<td>2010-04-14</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>G</td>
<td>US DoD</td>
<td>2010-03-16</td>
<td>2010-04-14</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>H</td>
<td>US Army</td>
<td>2010-03-16</td>
<td>2010-04-14</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>I</td>
<td>Autonomica</td>
<td>2010-03-15</td>
<td>2010-03-03</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>J</td>
<td>VeriSign</td>
<td>N/A</td>
<td>2010-05-05</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>K</td>
<td>RIPE NCC</td>
<td>2010-03-15</td>
<td>2010-03-24</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>L</td>
<td>ICANN</td>
<td>2010-03-15</td>
<td>2010-01-27</td>
<td>submitting</td>
<td>submitting</td>
</tr>
<tr>
<td>M</td>
<td>WIDE</td>
<td>2010-03-15</td>
<td>2010-03-03</td>
<td>submitting</td>
<td>submitting</td>
</tr>
</tbody>
</table>
Key Ceremonies

- Key ceremonies has been tested and exercised during January and February.
  - See Root Zone DNSSEC KSK Ceremonies Guide for more information.

- The secure facilities are being fine tuned to meet the requirements set by NTIA and the expectations set by the community.
TCR Proposal

• Draft document describing how recognized members of the DNS technical community could be part of the key management process has been published.

  ‣ See Trusted Community Representatives – Proposed Approach to Root Key Management for more information.
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 1-2 months before the validatable signed root zone is in production.
Policy Update

• An minor update of the DNSSEC Practice Statements (DPS) for the KSK and ZSK will be published shortly.

  ‣ Not much has changed, but please read this policy – 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
- Policy and Practice Statements
- Trust Anchor Publication
- Deployment Plan
- KSK Ceremonies Guide
- TCR Proposal
- Resolver Testing with a DURZ
Questions & Answers
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