DNSSEC for the Root Zone

MENOG 6 Riyadh, Saudi Arabia
April 2010

Mehmet Akcin, ICANN
This design is the result of a cooperation between ICANN & VeriSign with support from the U.S. DoC NTIA
Roles and Responsibilities
ICANN
IANA Functions Operator

- Manages the Key Signing Key (KSK)
- Accepts DS records from TLD operators
- Verifies and processes request
- Sends update requests to DoC for authorization and to VeriSign for implementation
DoC NTIA
U.S. Department of Commerce
National Telecommunications and Information Administration

• Authorizes changes to the root zone
  ‣ DS records
  ‣ Key Signing Keys
  ‣ DNSSEC update requests follow the same process as other changes

• Checks that ICANN has followed their agreed upon verification/processing policies and procedures
VeriSign
Root Zone Maintainer

- Manages the Zone Signing Key (ZSK)
- Incorporates NTIA-authorized changes
- Signs the root zone with the ZSK
- Distributes the signed zone to the root server operators
**DNS records** sent from TLD operator to ICANN

**Verified data** sent to DoC

**Authorized data** sent to VeriSign

**Root Zone** distributed to root servers

TLD Operator → **ICANN**

RZM → **DoC**

Unsigned root → **Signer** → Signed root → **Root Servers**

ZSK sent from VeriSign to ICANN

KSK published by ICANN

Keyset is signed by KSK and sent back from ICANN to VeriSign
Deployment
Goals

• Deploy a signed root zone
  ▸ Transparent processes
  ▸ Audited procedures
  ▸ DNSSEC deployment
    • validators, registries, registrars, name server operators

• Communicate early and often!
Anticipated Issues
DO=1

• A significant proportion of DNS clients send queries with EDNS0 and DO=1

• Some (largely unquantified, but potentially significant) population of such clients are unable to receive large responses

• Serving signed responses might break those clients
Rollback

• If we sign the root, there will be some early validator deployment

• There is the potential for some clients to break, perhaps badly enough that we need to un-sign the root (e.g., see previous slide)

• Un-signing the root will break the DNS for validators
Staged Deployment
Deploy Incrementally

- The goal is to leave the client population with some root servers not offering large responses until the impact of those large responses is better understood
- Relies upon resolvers not always choosing a single server
DURZ

- Deploy conservatively
  - It is the root zone, after all

- Prevent a community of validators from forming
  - This allows us to unsign the root zone during the deployment phase (if we have) to without collateral damage
DURZ

- “Deliberately Unvalidatable Root Zone”
- Sign RRSets with keys that are not published in the zone (but with matching keytag…)
- Publish keys in the zone which are not used, and which additionally contain advice for operators (see next slide)
- Swap in actual signing keys (which enables validation) at the end of the deployment process
. 3600 IN DNSKEY 257 3 5 (AwEAAa+.............................
++THIS/KEY/AN/INVALID/KEY/AND/SHOULD
/NOT/BE/USED/CONTACT/ROOTSIGN/AT/ICANN/DOT/ORG/FOR/MORE/INFORMATION+++++
++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
) ; Key ID = 6477
Deploy Incrementally

<table>
<thead>
<tr>
<th></th>
<th>Completed on 27 January</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>Completed on 10 February</td>
</tr>
<tr>
<td>M, I</td>
<td>Completed on 3 March</td>
</tr>
<tr>
<td>D, K, E</td>
<td>Completed March 22nd</td>
</tr>
<tr>
<td>B, H, C, G, F</td>
<td>Being Completed this week. “April 14th”</td>
</tr>
<tr>
<td>J</td>
<td>May 5th</td>
</tr>
</tbody>
</table>
Measurement

- For those root servers that are instrumented, full packet captures and subsequent analysis around signing events
- Ongoing dialogue with operator communities to assess real-world impact of changes
Testing

- A prerequisite for this proposal is a captive test of the deployment
  - Test widely-deployed resolvers, with validation enabled and disabled, against the DURZ
  - Test with clients behind broken networks that drop large responses
Interaction with TLDs
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

• Current topic of discussion within Root DNSSEC Design Team
Communication
Project Web Page

• http://www.root-dnssec.org
  ▸ Status updates
  ▸ Documents
  ▸ Presentation Archive
  ▸ Small collection of links to relevant tools
  ▸ Contact information
  ▸ RSS
Communication
with non-technical audiences

• Will reach the non-technical and semi-technical audiences with press releases and other means.

• PR departments with people who know how to do this will be engaged.
Communication
with technical audiences

• Reaching the technical audiences via mailing lists and other means
  ‣ IETF DNS lists (e.g. DNSOP)
  ‣ non-IETF DNS lists (e.g. DNS-OARC)
  ‣ General operator lists (e.g. MENOG)
  ‣ ...

Thursday, April 8, 2010
Draft Timeline

• December 1, 2009
  ‣ Root zone signed
    • Initially signed zone stays internal to ICANN and VeriSign
    ‣ ICANN and VeriSign begin KSR processing
    • ZSK and KSK rolls

• January - July 2010
  ‣ Incremental roll out of signed root

• July 1, 2010
  ‣ KSK rolled and trust anchor published
  ‣ Signed root fully deployed
Deployment Status

13 April 2010
Documentation

- Requirements document posted
- High-Level Architecture, Policy and Practice Statements, Trust Anchor Publication, Deployment documents posted in draft form
- Ceremony, KSK Facility Requirements, Testing documents expected to be posted soon

http://www.root-dnssec.org
Testing

- Data collection testing by Root Server Operators complete - have now done this for real
- Several KSR/SKR exchanges complete
- DURZ vs. Resolver testing complete
DURZ Roll-Out

- L, A, M, I, D, K, and E root servers are running the DURZ
- B, C, G, F, and H will complete the transition this week.
- J will have DURZ on 5 May 2010
Other zones

ARPA is now signed

Work on how to sign IN-ADDR.ARPA, IP6.ARPA is happening and reasonable progress is expected.
Thoughts?

- Feedback is extremely welcome
  - Email to rootsign@icann.org
Root DNSSEC Design Team

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