DNSSEC for the Root Zone – Update

IETF 78, Maastricht, The Netherlands
27 July 2010

Joe Abley, ICANN and 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)
Deployment Status

• **Done!**

• Full production on July 15, 2010
  ▸ Already had DURZ at every root server
    ▸ Keys became unobscured

• No problems reported
DS Record Change Requests

• DS record requests being accepted by IANA now
• TLD change template now includes DS records
• DS RRsets for bg, br, cat, cz, lk, na, org, tm, uk already in the root
Trusted Community Representatives (TCRs)

• Crypto Officers (CO)
• Recovery Key Shareholders (RKSH)
• Not from an organization affiliated with the root zone management process
  ▸ ICANN, VeriSign or the U.S. Department of Commerce
TCRs

- Crypto Officers (COs)
  - Have physical keys to safe deposit boxes holding smartcards that activate the HSM
  - ICANN cannot generate new key or sign ZSK without 3-of-7 COs
  - Able to travel up to 4 times a year to US
  - Don’t lose the (physical) key
TCRs

• Recovery Key Share Holders (RKSHs)
  – Have smartcards holding pieces (M-of-N) of the key used to encrypt the KSK inside the HSM
  – If both key management facilities fall into the ocean, 5-of-7 RKSH smartcards and an encrypted KSK smartcard can reconstitute KSK in a new HSM

• Backup KSK encrypted on smartcard held by ICANN
  – Able to travel on relatively short notice to US, but hopefully never

  – Annual inventory
<table>
<thead>
<tr>
<th><strong>Crypto Officers (COs)</strong></th>
<th><strong>Backup COs</strong></th>
<th><strong>Recovery Key Shareholders (RKSHs)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>U.S. East:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alain Aina, BJ</td>
<td>Christopher Griffiths, US</td>
<td>Bevil Wooding, TT</td>
</tr>
<tr>
<td>Anne-Marie Eklund Löwinder, SE</td>
<td>Fabian Arbogast, TZ</td>
<td>Dan Kaminsky, US</td>
</tr>
<tr>
<td>Frederico Neves, BR</td>
<td>John Curran, US</td>
<td>Jiankang Yao, CN</td>
</tr>
<tr>
<td>Gaurab Upadhaya, NP</td>
<td>Nicolas Antoniello, UY</td>
<td>Moussa Guebre, BF</td>
</tr>
<tr>
<td>Olaf Kolkman, NL</td>
<td>Rudolph Daniel, UK</td>
<td>Norm Ritchie, CA</td>
</tr>
<tr>
<td>Robert Seastrom, US</td>
<td>Sarmad Hussain, PK</td>
<td>Ondřej Surý, CZ</td>
</tr>
<tr>
<td>Vinton Cerf, US</td>
<td>Ólafur Guðmundsson, IS</td>
<td>Paul Kane, UK</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>U.S. West:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Andy Linton, NZ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carlos Martinez, UY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dmitry Burkov, RU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edward Lewis, US</td>
<td></td>
<td></td>
</tr>
<tr>
<td>João Luis Silva Damas, PT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Masato Minda, JP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subramanian Moonesamy, MU</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Backup RKSHs</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>David Lawrence, US</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dileepa Lathsara, LK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jorge Etges, BR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kristian Ørmen, DK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ralf Weber, DE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warren Kumari, US</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Key Ceremonies

• Ceremony #1: June 16, 2010, Culpeper, VA
  ▸ KSK created, Q3 root DNSKEY RRsets signed
  ▸ Recovery Key Shareholders and East Coast Crypto Officers enrolled

• Ceremony #2: July 12, 2010, Los Angeles, CA
  ▸ KSK installed, Q4 root DNSKEY RRsets signed
  ▸ West Coast Crypto Officers enrolled
Key Ceremony Video

• To be inserted here
DURZ/DITL Data

• Nine separate data collection events
• Usually 48 hours (most recent was 120 hours)
• DNS Queries only
• Some 20TB of data
• Asked all root operators to participate
UDP Query Rate

2010-01-19 Pre DURZ
2010-01-27 L DURZ
2010-02-10 A DURZ
2010-03-03 I,M DURZ
2010-03-24 D,E,K DURZ
2010-05-05 J DURZ
2010-05-25 Post DURZ
2010-07-14 Validating
DNSSEC Query Types
For A-root
TLDs of DS Queries

(Based on data from 2010-07-14 through 2010-07-19)
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