DNSSEC Update

Mehmet Ackin
Critical Infrastructure Engineer
ICANN

Presented by:
Baher Esmat
Manager, Regional Relations - Middle East

APTLD Meeting
Amman, Jordan
1 Nov, 2010
Signing the Root

The project has been coordinated by ICANN and VeriSign with support from DoC/NTIA
ROLES AND RESPONSIBILITIES
ICANN: IANA Function’s Operator

- Manages the Key Signing Key (KSK)
- Accepts DS records from TLD operators
- Verifies and processes request
- Sends update requests to DoC/NTIA for authorization and to VeriSign for implementation
DoC/NTIA

- Checks that ICANN has followed their agreed upon verification/processing policies and procedures
- Authorizes changes to the root zone
  - DS records
  - Key Signing Keys
  - DNSSEC update requests follow the same process as other changes
VeriSign

- 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
DESIGN
The guiding principle behind the design is that the result must be trustworthy.
Transparency

Processes and procedures should be as open as possible for the Internet community to trust the signed root
Processes and procedures should be audited against industry standards,

e.g. ISO/IEC 27002:2005
DNSSEC Practice Statement (DPS)

• States the practices and provisions that are employed in root zone signing and zone distribution services
  – Issuing, managing, changing and distributing DNS keys in accordance with the specific requirements of the U.S. DoC NTIA

• Third-party auditors check that ICANN operates as described in the DPS
High Security

Root system should meet all NIST SP 800-53 technical security controls required by a HIGH IMPACT system
Physical Security

- Facility – Tier 1: Access control by Facility Operator
- Facility – Tier 2: Access control by Facility Operator
- Man Trap – Tier 3: Access control by ICANN
- Key Ceremony Room – Tier 4: Access control by ICANN
- Safe Room – Tier 5: Access control by ICANN
- Safe #1 – Tier 6
  - HSM – Tier 7
    - Private Keys
  - Key Ceremony Computer
- Safe #2 – Tier 6
  - Safe Deposit Box – Tier 7
    - Crypto Officers’ Credentials
Physical Security

- Restricted Area
- Authorized Personnel Only

- Notice: All employees and visitors must wear identification badges
- Notice: Unauthorized persons not permitted beyond this point
- Notice: No food or drink beyond this point
- Notice: Turn off cellular phones, pagers and other wireless devices
- Notice: No firearms or weapons allowed on this property
Community Involvement

*Trusted representatives from the community are invited to take an active role in the key management process*
Trusted Community Representatives (TCRs)

- Have an active role in the management of the KSK
  - as Crypto Officers needed to activate the KSK
  - as Recovery Key Shareholders have pieces of the key that encrypts the backup copy of the KSK
Crypto Officer (CO)

- 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
Recovery Key Shareholder (RKSH)

- 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 reconstituted KSK in a new HSM
- Backup KSK encrypted on smartcard held by ICANN
- Able to travel on relatively short notice to US
<table>
<thead>
<tr>
<th>CO</th>
<th>CO Backup</th>
<th>RKSH</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Alain Aina, BJ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Anne-Marie</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Eklund Löwinder, SE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Frederico Neves, BR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Gaurab Upadhaya, NP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Olaf Kolkman, NL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Robert Seastrom, US</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Vinton Cerf, US</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 Luís 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>- Christopher Griffiths, US</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Fabian Arbogast, TZ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- John Curran, US</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Nicolas Antoniello, UY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Rudolph Daniel, UK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Sarmad Hussain, PK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Ölafur Guðmundsson, IS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Bevil Wooding, TT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Dan Kaminsky, US</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Jiankang Yao, CN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Moussa Guebre, BF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Norm Ritchie, CA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Ondřej Surý, CZ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Paul Kane, UK</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>
Deliberately Unvalidatable Root Zone (DURZ)

- A method to allow conservative and controlled deployment of DNSSEC to the root
- Main purpose is to measure effect on normal DNS resolutions
- Deploy incrementally in the root (Jan-10 to May-10)
Root Signing

• June 2010
  • First ceremony in Culpeper, Virginia
    • Created initial root zone KSK
    • Q3/2010 ZSK signing request (KSR) processed
  • First DS records added to the root zone

• July 2010
  • Second ceremony in Los Angeles, California
    • Key material from the first ceremony replicated and stored
    • Q4/2010 KSR processed
    • Live streamed to the world
  • The fully validatable signed root zone is published to the root servers by VeriSign
Key Ceremony
Key Ceremony
Communications

• Mailing lists
  • IETF DNS lists (e.g. DNSOP)
  • non-IETF DNS lists (e.g. DNS-OARC)
  • General operator lists (e.g. NNNOG)

• Project website
  • http://www.root-dnssec.org
The root is signed!

TLD operators can submit DS records to the IANA for inclusion in the root zone

http://www.iana.org/procedures/root-dnssec-records.html
Questions?