DNSSEC for the Root Zone

ICANN 36, Seoul
28 October 2009

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
Design Requirements
Keywords
Transparency

Processes and procedures should be as open as possible for the Internet community to trust the signed root
Audited

Processes and procedures should be audited against industry standards, e.g. ISO/IEC 27002:2005
High Security

Root system should meet all NIST SP 800-53 technical security controls required by a HIGH IMPACT system
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
• 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
**VeriSign**

- **TLD Operator** sends **DNS records** to **ICANN**
- **ICANN** sends **RZM** to **DoC**
- **DoC** sends **Verified data** to **VeriSign**
- **Authorized data** sent to **VeriSign**
- **ZSK** sent from **VeriSign** to **ICANN**
- **KSK** published by **ICANN**
- **Keyset** is signed by **KSK** and sent back from **ICANN** to **VeriSign**
- **ZSK** sent from **VeriSign** to **ICANN**
- **Signed root** sent to **Root Servers**
- **Root Zone** distributed to **root servers**
Proposed Approach to Protecting the KSK
**Physical Security**

<table>
<thead>
<tr>
<th>Tier</th>
<th>Description</th>
<th>Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Facility</td>
<td>by Data Center</td>
</tr>
<tr>
<td>2</td>
<td>Facility</td>
<td>by Data Center</td>
</tr>
<tr>
<td>3</td>
<td>Facility</td>
<td>by Data Center</td>
</tr>
<tr>
<td>4</td>
<td>Cage</td>
<td>by Data Center</td>
</tr>
<tr>
<td>5</td>
<td>Safe Room</td>
<td>by ICANN</td>
</tr>
<tr>
<td>6</td>
<td>Safe #1</td>
<td>by Tier 6</td>
</tr>
<tr>
<td>7</td>
<td>HSM</td>
<td>by Tier 7</td>
</tr>
<tr>
<td></td>
<td>Private Keys</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Key Ceremony Computer</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Safe #2</td>
<td>by Tier 6</td>
</tr>
<tr>
<td></td>
<td>Safe Deposit Box</td>
<td>by Tier 7</td>
</tr>
<tr>
<td></td>
<td>Crypto Officers’ Credentials</td>
<td></td>
</tr>
</tbody>
</table>
DPS
DNSSEC Policy & Practice Statement

• 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

• Comparable to a certification practice statement (CPS) from an X.509 certificate authority (CA)
Key Signing Key Management

ICANN Staff
External Trusted Persons
Generate
Publish
Use
Destroy

Other Witnesses
3rd Party Auditors
Policy & Practice Statement

Zone Signing Key Management

VeriSign Staff
Generate
Publish
Use
Destroy

Other Witnesses
3rd Party Auditors
Policy & Practice Statement

Global Internet Community
3rd Party Auditors
Community Trust

- Proposal that community representatives* have an active roll in management of the KSK
  - as Crypto Officers needed to activate the KSK
  - as Backup Key Share Holders protecting shares of the symmetric key that encrypts the backup copy of the KSK

*) drawn from members of entities such as ccNSO, GNSO, IAB, RIRs, ISOC
Auditing & Transparency

- Third-party auditors check that ICANN operates as described in the DPS
- Other external witness may also attend the key ceremonies
Proposed DNSSEC Protocol Parameters
Key Signing Key

• KSK is 2048-bit RSA
  ▸ Rolled every 2-5 years
  ▸ RFC 5011 for automatic key rollovers

• Propose using signatures based on SHA-256
Zone Signing Key

• ZSK is 1024-bit RSA
  ▸ Rolled once a quarter (four times per year)

• Zone signed with NSEC

• Propose using signatures based on SHA-256
Signature Validity

- DNSKEY-covering RRSIG validity 15 days
  - re-sign every 10 days
- Other RRSIG validity 7 days
  - re-sign twice per day (with zone generation)
Key Ceremonies

• Key Generation
  ‣ Generation of new KSK
  ‣ Every 2-5 years

• Processing of ZSK Signing Request (KSR)
  ‣ Signing ZSK for the next upcoming quarter
  ‣ Every quarter
Root Trust Anchor

• Published on a web site by ICANN as
  ▸ XML-wrapped and plain DS record
  ▸ to facilitate automatic processing
  ▸ PKCS #10 certificate signing request (CSR)
    • as self-signed public key
    • Allows third-party CAs to sign the KSK
Proposed Deployment
Roll Out

- Incremental roll out of the signed root
  - Groups of root server “letters” at a time
- Watch the query profile to all root servers as roll out progresses
- Listen to community feedback for any problems
No validation

- Real keys will be replaced by dummy keys while rolling out the signed root
  - Signatures will not validate during roll out
  - Actual keys will be published at end of roll out
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**
Thoughts?

• Feedback on this proposal would be extremely welcome
  ‣ Here in room
  ‣ Email Rick or Matt
Root DNSSEC Design Team

Joe Abley
David Blacka
David Conrad
Richard Lamb
Matt Larson
Fredrik Ljunggren
David Knight
Tomofumi Okubo
Jakob Schlyter