ICANN proposal to sign the root

ICANN DNSSEC Workshop
November 5, 2008, Cairo
Dr. Richard Lamb
richard.lamb@icann.org
DNSSEC...

• ...protects the lookup like HTTPS/SSL protects the “conversation”

• ...is about security – not control. Does not change control. Does not effect existing applications

• ...is a PKI for DNS

• ...if secured and trusted, is a global platform for innovation
Recent Events

- Calls from the community to sign the root: RIPE, SE, ORG, UK, APNIC + press
- **.se** signs their zone. Leads the way and is an example for others to do so. (2/2007)
- BR, BG, PR, CZ, MUSEUM sign their zones. Upcoming: ORG, GOV, UK, CA, ...
- So...in close cooperation with DNSSEC deployment and security experts (.SE, .UK, IETF) developed signing system for .arpa and root. Signed root publicly available at ns.iana.org (and anycast pch-test.iana.org) for well over a year (6/2007)
- Presentations describing system and seeking feedback at various fora: IETF, RIPE, ICANN, OARC, etc..
- DNSSEC and root zone management are part of ICANN Strategic Plan – primary part of IANA function and ICANN business
- DNSSEC @ ICANN paper published (7/24/2008)
- Interim-TAR (almost there), Root Zone Management system (ongoing)
- Dan Kaminsky! (8/5/2008)
- US Government mandates DNSSEC for its own .gov use (8/22)
- ICANN submits proposal to sign the root (9/2)
- NTIA response (9/9) (http://www.icann.org/correspondence/ )
- VeriSign submits proposal (9/22)
- Market crashes (10/1), Industry meeting on DNSSEC in DC
- NTIA announces 45-day NOI on signing the root (10/9) - end 11/24
ICANN’s root signing proposal

• No change in current control
• Accept no compromises in security
• Designed by Community for Community
• No one organization controls the key
• Regular auditing and reporting
• Timely deployment building on existing signed root and experience
• Maximum reliability through automation
• Flexible to support evolving landscape
• All Open Source
Elements of root signing

• Important elements of a root-signing solution are transparency, public consultation, broad stakeholder participation (e.g. key ceremony), flexibility, reliability, and trust;

• Solution has to balance various concerns, but must provide for a maximally secure technical solution and one that provides the trust promised by DNSSEC;

• An open, transparent and international participatory process will allow for root zone management to adapt to changing needs over time as DNSSEC is deployed throughout the Internet and as new lessons are learned.
Trust
preservation of trust from TLD operator to signed root

• PKI overlaid on DNS - treat it like one.
• A chain of trust
• Only as trustworthy as weakest link
• Intense pressure on root “link”
• A platform for innovation
.....if done right
Trust the root key

• Anyone can generate keys and sign the root
• The resultant signed root has no value unless those it will serve agree to trust and use the key that signed it
• Publication of (the public half of) the key and attestation to the process, procedure, and equipment that generated it by the global Internet community gives it this value
• Classic cooperative definition for the Internet
• Broad stakeholder participation, e.g., Key Ceremony
• No one organization controls the key
• Balanced with stability and security
Overview

Key Ceremony
- HSM 1: Generate KSK
- HSM 2: Sign Keyset
- HSM 3: Generate ZSK
- Sign Zone /w ZSK

Distribute Zone

Keyset

IANA
- Physically co-located with IANA to ensure security but not controlled by ICANN/IANA
- Digitally Signed (protected) Root Zone

TLD Operator
- Established trust relationships
- Physically co-located

Auditor
- Content Authorize and Audit
- Physically co-located

Root Zone Distributor
- A
- M
Capabilities

- Sophisticated L – root operations
- Comprehensive Registry Failover processes and procedures
- Root zone management is our business.
- DNSSEC is part of ICANN’s Strategic Plan and budget
- Signed .arpa and root system developed closely with DNSSEC experts and publicly testing since June 2007
- Interim Trust Anchor Repository for TLDs
- Root zone management system
- Skilled staff
Preparedness

• IANA’s signed root was developed closely with DNSSEC experts and based on Sweden’s production .se deployment. Publicly available and testing for well over a year at ns.iana.org (and others)
• Collaboration and development with DNSSEC deployment and security experts has been a continual process as part of signing Internet infrastructure zone .arpa at the request of the IAB
• Original crypto interface (PKCS11) development to support flexible HSM usage shared with community. All DNSSEC work will be Open Source.
• IANA has deployed only the highest security (FIPS 140-2 Level 4) HSMs used by UN treaty organizations
• Developed sample Key Ceremony and other key management approaches with expert security engineering help to balance security, stability, and participation
• Operations in secure facilities (multiple biometrics, secure containers, etc.)
• ...the list goes on but it is not our place to tell the community what to do. ICANN serves the community. So the community must tell us what to do. Public consultation and participation are key parts of the ICANN proposal.
Behind our testbed

SIGNER, NS:
DELL 1950 /w
2xPS, 2XSAS,
2xCPU

HSM: AEP
KEYPER FIPS
140-2 Level 4
(Disposable)

HSM KSK
10.0.2 X
SIGNER
10.0.1 X
SIGNER

HSM ZSK
NS
199.7.81.10

NS
199.7.81.15

CLASS 5 GSA
NSA SAFE

ROOT DB

ADMIN

RZM

I-TAR

TSIG
2-factor auth for RZM

F/W

24 hr manned
multiple biometric
controlled facility,
NSA NSTISSP #10,
GSA Class 5
Container
(approved for Top
Secret)

ns.iana.org
208.77.188.32

pch-test.iana.org
Anycast
204.61.216.37

TEST A

TEST M

MONITORING SITES

BOS
MIA
AMS
LAX

TLD OPERATORS

TLD DATA
VETTING
PROCESS

TLD OPERATORS
AND/OR
GOVERNMENTS

EXISTING TRUST
RELATIONSHIPS

149.20.64.22 public
recursive resolver

iana-testbed.odvr.dns-oarc.net

System status at: https://ns.iana.org/dnssec/status.html
.arpa, in-addr.arpa, ip6.arpa, iris.arpa, urn.arpa, uri.arpa,
.int, xn-"test" (DS: .se, .br, .bg, .pr, .cz, .museum.)
To test using this demo (nameserver ns.iana.org) refer to the sample BIND configuration file [here](https://ns.iana.org/dnssec/status.html). Note: This data, including the signed zones, are purely for test purposes and are not to be used in any production capacity. We do not guarantee their availability, and they may not always function correctly.

<table>
<thead>
<tr>
<th>ZONE (serial)</th>
<th>STATE LAST UPDATED</th>
<th>VALIDITY PERIODS (keyid)</th>
<th>EFFECTIVITY PERIODS (keyid)</th>
<th>TRUST ANCHORS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>test</strong></td>
<td>Ok</td>
<td>2008-SEP-24 16:25:49</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2008-SEP-02</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2008-OCT-15</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2008-DEC-31</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(46716 Z9K)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

AQOKgIN...

IN DNSKEY 257 3 5 (AKMW2011F0D1.Pb+snq841bEPt2kPressv917c8jcbIoxt39tE9MCDEccFrq+Kf15pS0L1+c0q8qVaFAsq8y6nIMTTlpmw6KGTq287Kc1KF
YWX7K2v6y5ndK2KtC/q6ZQd4cYbYVQ0Df1bLYm
Aq6b963Yx7T2Z1377214a33Q/17y/6aXW+13a
?c3c3cThjCNgf+H01nG9npG6Gip3d54c65y51+
DkVvU7XpQpqaq90KjAyfl7/Ar1222UM2H2U6pL
qlkT4c0dCT/58YTeE619y+1QP1hmHIgEy15a
P5h22UZ2a58n5b52b52NmI5N9P33UpU4508u
AruRaqTBrL275Wv/EpKgC51C=

| key id | 4183 |

IN DNSKEY 257 3 5 (AKMW2011F0D1.Pb+snq841bEPt2kPressv917c8jcbIoxt39tE9MCDEccFrq+Kf15pS0L1+c0q8qVaFAsq8y6nIMTTlpmw6KGTq287Kc1KF
YWX7K2v6y5ndK2KtC/q6ZQd4cYbYVQ0Df1bLYm
Aq6b963Yx7T2Z1377214a33Q/17y/6aXW+13a
?c3c3cThjCNgf+H01nG9npG6Gip3d54c65y51+
DkVvU7XpQpqaq90KjAyfl7/Ar1222UM2H2U6pL
qlkT4c0dCT/58YTeE619y+1QP1hmHIgEy15a
P5h22UZ2a58n5b52b52NmI5N9P33UpU4508u
AruRaqTBrL275Wv/EpKgC51C=

| key id | 34291 |
Go ahead – test it

• Recursive public DNSSEC resolver at 149.20.64.22 (iana-testbed.odvr.dns-oarc.net). Thank you OARC!

• Masters: 208.77.188.32 (ns.iana.org) and anycast 204.61.216.37 (pch-test.iana.org). Thank you PCH!
• Congratulations. A good read! Overall a pretty fair and accurate treatment of the issue.
• However absent throughout the text and flow diagrams is the representation of the trust from TLD operator to signed root. (e.g. the multiple levels of TLD key vetting and validation and the incorporation of those keys into the signed root).
• VeriSign and ICANN proposals published in their entirety
• Comments from all stakeholders in the global Internet community will make a difference!
Comparison of proposals

• ICANN
  – No restrictions on design
  – IANA vets TLD keys and immediately signs zone file
  – DNSSEC experts from community design final system, including KSK handling, for ICANN to implement
  – Community determines “who, how, where”. Design by the community for the community.

• VeriSign
  – IANA vets TLD keys and transmits keys to VeriSign who signs zone file
  – M of N KSK handling by 12 root server operators
  – Assumes IANA cannot create zone file
What’s Missing in the NOI

Proposed Process Flow No. 1

What about security and trust here??
A chain of trust (ICANN proposal)
...an extra link in the chain

- root trust anchor
- zone signing organization
- TLD keys over link
- vet only (IANA)
- TLD
- 2nd level domain
- key for link
• Why add another link?

• An avenue for key corruption.

• Who has key to this link?

• How is that key managed?

• Would you trust your savings to this?

• Keep it simple
Summary of ICANN’s root signing proposal

- No change in current control
- Accept no compromises in security
- Designed by Community for Community
- Timely deployment building on existing signed root and DNSSEC expert experience
- Flexible and open as DNSSEC evolves – in technology and policy
It's your root

• Help design it

• Help test it

• Help run it

• Make it a trusted platform for innovation

• Your feedback counts! Comment to the NOI!
Interim Trust Anchor Repository

- What is an ITAR?
- Interim Trust Anchor Repository
- A mechanism to publish keys of top-level domains that currently implement DNSSEC
- When the root zone is DNSSEC signed, such a repository is unnecessary
- Therefore this is a stopgap measure
- Should be decommissioned when the root is signed
Publishing formats

• Publication formats
  – List on website
  – XML structured format
  – Master file format

• Should work with major software implementations

• Formats are plain text and readable so implementers can modify to suit

• Implementers should not be putting special ITAR provisions in code — this is meant to go away when the root is signed!
Availability

- Open to top-level domain operators in a week or two
- Asked to play with it for a week or so, try revoking etc.
- System will then be reset to contain only valid records
- Open to general public once TLD operators who sign have opportunity to list keys
- Expected in a few weeks
Thank you
and
This was not done alone! Thanks to the many experts from the Internet community!!

Questions?