DNSSEC @ IANA

NANOG 44
October 14, 2008, Los Angeles
richard.lamb@icann.org
DNSSEC is …

• a PKI

• SSL for DNS without encryption
Recent Events

• Calls from the community to sign the root. RIPE, SE, ORG, UK, APNIC…press
• TLD’s sign their zones SE, BR, BG, PR, CZ, MUSEUM. Announced: 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 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 – a primary part of our business
• DNSSEC @ ICANN paper published (7/24)
• Interim-TAR (almost there), Root Zone Management system (ongoing)
• Kaminsky (8/5)
• 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
A good read! Overall a pretty fair and accurate treatment of the issue.

Flow 4 is our proposal. Flow 5 is VeriSign’s.

Oddly absent throughout the text and flow diagrams are the processes of authenticating TLD keys and the transfer of those keys to the editing process. Elsewhere in the diagrams any transfer of keys between processes are both described in the text and specifically annotated in the diagrams.

VeriSign and ICANN proposals published in their entirety

Need your technical feedback
What about these keys??

Proposed Process Flow No. 1

- TLD Operator
  - Change Request
    - Process Change Request
      - IANA Functions Operator
        - Verify Authorize Change Request
          - Administrator
            - Verify Authorize Key Update Request

- Root Key Operator
  - Sign Root Keyset
  - Generate KSK

- Root Zone Maintainer
  - Generate ZSK
  - Sign Zone
    - Distribute Zone File

- Root Server Operators
  - A, B, C, M
    - Distribute Public Key to DNS Community

- Transmit Public Key
- Transmit Private Key
- Key Update Request
proposals to sign the root

• 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”

• VeriSign
  – Assumes IANA cannot create zone file
  – IANA vets TLD keys and transmits keys to VeriSign who signs zone file
  – M of N KSK handling by root server operators
Anyone can sign the root and generate keys
A KSK has no value unless everyone agrees to trust and use it
Classic cooperative definition for the Internet
Community trust in:
  - how it is generated and protected
  - by whom and how it is used
  - how it is published and attested to
  - how auditing + reporting are performed
In any case: ZSK signer can sign anything
part of a chain of trust / PKI

- PKI overlaid on DNS
- Treat it like one.
- A chain of trust
- Only as trustworthy as weakest link
- Pressure on root “link”
- A platform for innovation
  …..if done right
dnssec chain of trust

root trust
anchor

vet+sign (IANA)
TLD

2\textsuperscript{nd} level
domain
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
“key” questions

• Delicate balance of control vs security vs stability
• trade offs:
  – ZSK signer can always modify content
  – KSK signing ability and lifetime
  – ZSK lifetimes/length
  – compromise recovery
  – trust in ZSK and KSK generation
  – key backup, backup sites
  – broad multi-stakeholder participation (e.g. Key Ceremony)

➤ Requirement: Flexibility in processes and design as DNSSEC experience evolves
overall considerations

- Trust
- Accountability to the community
  - root zone management is IANA’s primary job
  - committed: Part of Strategic Plan and Budget.
  - dnssec operations considered and envisioned for some time
- Transparency
  - system design help from experts in the Internet community which it would serve
  - roles: “Who and where” would be chosen by community
  - regular auditing and reporting to and by community
  - open source
- Timeliness
  - been operational over a year (June 2007)
  - preparedness efforts continue to serve if asked
  - dedicated funding and staff
- Reliability
  - multiple redundant systems at each site and backup/mirror sites
  - expertise from outside and in house (registry failover processes, sophisticated L-root operations)
- Flexibility
  - experts can re-arrange “the pieces” to meet changing requirements
  - native pkcs11 support designed in for HSM transitions
  - regular participation in a broad set of meetings and discussions IETF, ccTLD, dnssec-deployment, ICANN, per-TLD dns and dnssec meetings to understand changing requirements
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.
Preservation of Trust

- Maintain trust from TLD operator to signed root. Any chain is only as strong as its weakest link.
- Increased confidence in DNS will depend more on this chain.
- Eliminate avenues for potential corruption during transmission between organizations.
- Keys (DS) should not have to go to another organization before being protected by signing.
- So the validator of changes signs the zone. A conclusion other DNSSEC deployers have come to.
- Will allow for timely and accurate TLD key replacement in the face of compromise
- Introduction of new gTLDs will stress this link
Transparency

- Open and transparent process for technical infrastructure design and signing oversight functions.
- KSK’s not under control of one organization.
- No security through obscurity: open source and designs.
- Continuous collaboration with DNSSEC experts to evolve design as lessons are learned.
- Regular auditing and reports.
Preparedness

- IANA’s “business” is root zone management. DNSSEC is part of ICANN’s Strategic Plan.
- IANA signed root was developed closely with DNSSEC experts. Publicly available for 15 months.
- Interim-TAR during the testing period (almost done)
- RZM would be modified to be ready to handle DS records incorporating technology and lessons from I-TAR
- Automation: signing, ZSK rollover (to avoid costly risk of service failures and errors), monitoring, notifications
- Kept the process and design simple
- Final design and ongoing modifications would be based on public consultation process with experts
- Plan on regular audits and reports on system operation and security
Key Ceremony

- Keys are not under the control of a single organization. IANA is key custodian only.
- Fresh key generation hardware each KSK gen. Dispose or recycle old.
- Community decides how, where, when, and who
- Any Interested stakeholders, auditors, publishers. Key has value only when witnessed and published by all.
- Filmed and broadcast
- Keys cannot be extracted, cloned or otherwise. Private key in FIPS 140-2 level 4 HSM (used by UN treaty org, etc). Key never leaves HSM. Tamper attempt destroys contents.
- Backup HSM’s configured during Key Ceremony
- Community decides how, where, and who for backup and disaster recovery
- Other schemes using other equipment (e.g., M of N) supported via PKCS11 standard interface.
Behind ns.iana.org

System status at: https://ns.iana.org/dnssec/status.html

-arpa, in-addr.arpa, ip6.arpa, iris.arpa, urn.arpa, uri.arpa, .int, .se, .br, .bg, .pr, .cz, .museum, xn.“test”.

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

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

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

- Maintainability – if it's not easy, it will fail. Automation is “key”!
- Reliability – if there is a problem, no one will use it
- Security – it must look and be secure for people to trust it. Preserve the trust
- For .arpa, in-addr.arpa, ip6.arpa, iris.arpa, urn.arpa, uri.arp as well (as per IAB).
Maintainability – Only Two Scripts

- **zsign**: automatically run daily on multiple machines to pickup zone changes (based on SOA serial, new DS records, or expiring signatures); reload hidden master; check key status; update status web page; and email notifications.

- **kgen**: automatically run daily to introduce new keys and generate signed key bundles if needed. Generates or uses pre-generated (attested to) keys.
Maintainability – Overlapping Keys, Rollover Script

- Multiple overlapping keys (effectivity periods) to simplify rollovers.
- ZSK - three (3), old-active-new, overlapping ZSKs /w staggered effectivity periods. Use currently “active” key to sign records
- KSK - two (2) overlapping KSKs /w staggered effectivity periods. Use both to sign “key bundle” of five (5) keys
- Key introduction and rollover automated

<table>
<thead>
<tr>
<th>Key Index File:</th>
</tr>
</thead>
<tbody>
<tr>
<td>dn</td>
</tr>
<tr>
<td>root KSK 005 64000</td>
</tr>
<tr>
<td>root KSK 005 24000</td>
</tr>
<tr>
<td>root ZSK 005 24001</td>
</tr>
<tr>
<td>root ZSK 005 08000</td>
</tr>
<tr>
<td>root ZSK 005 92000</td>
</tr>
</tbody>
</table>
Maintainability – Compromised Key, Replacement Script

• For bad ZSK (old, active, new keys)
  – old – replace key with newly introduced “old” key.
  – active – use old key to sign and introduce a replacement. Phase out bad key.
  – new – replace key with “new” key.
  – Normally done in one-step. Two-steps if “close” to a transition to account for DNS propagation delays.

• For bad KSK (2 keys)
  – One - replace key with new KSK (from pre-generated keys) with the same effectivity period and immediately publish.
  – Both – introduce two new keys and phase out bad keys (tbd: may want to exercise rfc5011 revoke bit).

• Process automated with badkey script
Reliability – Dual Signers

- Design: Two (2) commodity hardware based SIGNERs, per site, periodically executing `zsign` to make sure the zone gets signed by one of them.
- Redundant hardware
- Backup sites (tbd)
Security – HSM

- To protect against internal as well as external attacks, generation, and signing is performed inside the HSM.
- Do this using modified BIND tools with native PKCS11 support
- FIPS 140-2 Level 4 devices (used by UN treaty org, credit card companies, military, etc)
- Top secret certified IPS GSA class 5 container
- 24 hour guarded, multiple biometric access controlled facility
Security – Key Lifetimes

- New ZSK 1024 bit every month to frustrate key guessing
- New KSK 2048 bit every year to frustrate key guessing
- Two KSKs always valid to support orderly replacement of old or compromised KSK
- Three published ZSKs to support orderly replacement and promotion of old or compromised ZSK
- 6 day (short) ZSK signature validity period to limit replay attacks while providing some time to recover from severe signing equipment failure
- 1.5 month key bundle KSK signature validity period to constrain compromised ZSK effects while not requiring daily manual resigning with KSK
Software

All software and modifications will be available as open source

SIGNERs
• kgen, badkey, and support programs
• pkcs11-backup, pkcs11-changepin, pkcs11-encrypt, pkcs11-random
• pkcs11 modified BIND tools: dnssec-signzone and dnssec-keygen
• zsign and support programs

Misc
• upsite – DNSSEC status web page generator
Add a Trust Anchor

Top-level domain operators who have used DNSSEC to sign their zones are invited to list their trust anchors in IANA's Interim Trust Anchor Repository. To successfully list a trust anchor, both the administrative and technical contacts for a domain must consent to the listing (as listed in IANA's root zone database). Matching DNSKEYs are also required to be in the secure domain's zone, however this does not need to be done straight away.

**Applicant**

Please provide the DNSSEC-signed domain to be listed in the repository. You may also provide and email address so that we may communicate to you the status of your request, as well as ask for any additional information.

- **Secured Domain**: 
- **Contact Email**: This email address will be informed of updates to this request.

**Trust Anchor Details**

The trust anchor itself is comprised of the attributes of a Delegation Signer (DS) key. These components are derived from the key that is used to sign the zone.

- **Key Tag**: The key tag of the trust anchor to be listed.
- **Key Digest**: The complete key digest of the trust anchor to be listed.
- **Key Algorithm**: The encryption algorithm used to compute the key.
- **Digest Type**: The hash digest algorithm used to compute the trust anchor.

**Listing Details**

These periods are used to determine how and when the trust anchor is listed in the repository. Typically keys are only used for discrete periods of time, with multiple keys overlapping in validity. These keys will help plan the listing of the keys in the repository. Dates can be entered in a number of formats, such as YYYY-MM-DD or YYYY-MM-DD HH:MM:SS.

- **Effectivity Period**: From [ ] Until [ ] The period the key will be valid for.
- **Listing Period**: From [ ] Until [ ] The period to list the key in the trust anchor repository.
- **Listing Password**: Protects this listing from revocation from those who do not know this password.

**Review Form**

Please review the material supplied above. Once you are happy with the supplied data submit the form and the details will be verified.

- **Submit**: Submit these details for verification.
- **Cancel**: Cancel the listing process.
## DEMO DNSSEC STATUS

To test using this demo (nameserver ns.iana.org) refer to the sample BIND configuration file [here](#).

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 otherwise function from time-to-time.

<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>root</td>
<td>(200809244D)</td>
<td>2008-SEP-24 16:25:49</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Hash: SHA1

```
$ORIGIN .
1  IN  DNSKEY 257 3 5  
    AvEAAhWMF0ULP+2m84IbEpz2kPqess9lC 
    cSt+jabLc05x3929ECic0q7xRT1pS01+C 
    0cvutVAsg8Vht0IM1rty56Htq267GciEf 
    YxXS2y66nKHb/CQ8Z9d-4ryXgV0o681bAm 
    bVdX00dVyt727f714a3SQ/17/0tX1j3 oA 
    qSc0h7jCk59H010R9mp06GjPn6Iud32ogY51+ 
    0VvVuE7XPQpzaq068KAYm7/0h2Kwdf6w064L 
    glqT4cdCT/88Y7eE461I9+vCG1h5mH1yEqy15R 
    F9k2UXa58w6vBvZSTzN0UpNPWQzEPwP0450U 
    Aqr54q5rB9r7uSw/EpKgC5IC= | ; key id = 4183 |
```
its your root

• Help us design it

• Help us test it

• Make it a trusted platform for innovation

• If you want a signed root, keep your foot on the gas pedal
Wasn’t done alone: Thanks to: Patrik Falstrom, Olaf Kolkman, Roy Arends, Jakob Schlyter, John Dickinson, David Soltero (.pr), David Conrad, Don Davis, David Miller, and so many others …

Thank you for listening

Questions ?