# ICANN's Preparedness for Signing the Root

September 24, 2008

DNS OARC Meeting, Ottawa, CA

richard.lamb@icann.org

# DNSSEC Activity

- Calls from the community to sign the root.
- TLD's sign their zones
- Close cooperation with DNSSEC deployment and security experts to develop signing system for .arpa and root
- Signed root publicly available at ns.iana.org for over a year
- Presentations describing system and seeking feedback at various fora
- 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), RZM (ongoing)
- Kaminsky (8/5)
- ICANN submits proposal to sign the root (9/2)
- NTIA response (9/9) http://www.icann.org/correspondence/

# 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

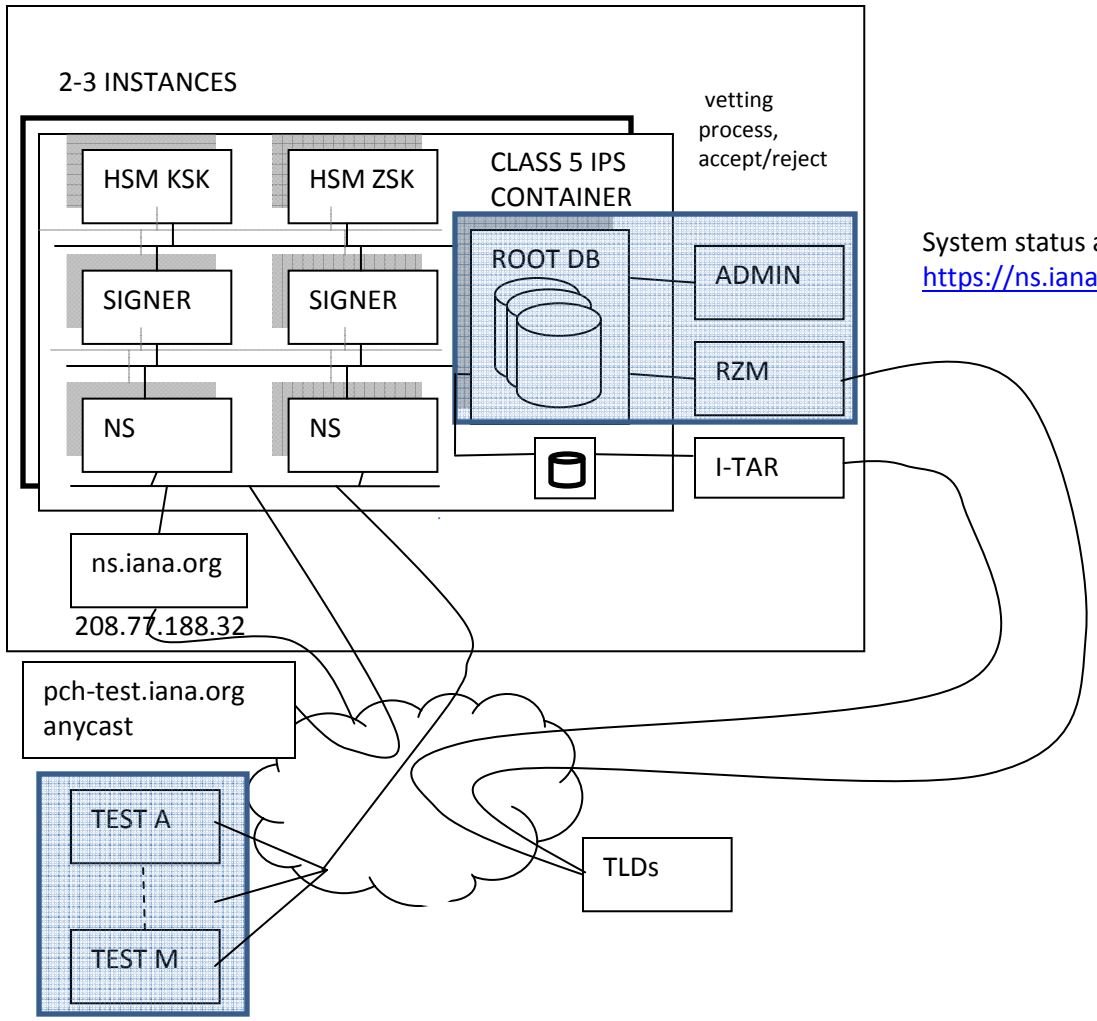
# Transparency

- 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! delayed by very effective TLD recursive resolver and patch effort – thank you Kim+OARC+operators!)
- 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

# Behind ns.iana.org




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

SIGNER, NS,
ROOT DBs: 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 Safe (approved for Top Secret)

# 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.

# 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**
The interim trust anchor repository is limited to top-level domains such as "COM" and "SE".

**Contact Email** (optional)
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** RSA/SHA-1
The encryption algorithm used to compute the key.

**Digest Type** SHA-1
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 validility. These times 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** (optional)
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.

| ZONE (serial) | STATE / LAST UPDATED | VALIDITY PERIODS (keyid) | EFFECTIVITY PERIODS (keyid) | TRUST ANCHORS |
|---|---|---|---|---|
| root (2008092440) | Ok 2008-SEP-24 16:25:49 | 2008-SEP-02 2008-OCT-15 (04183 KSK)<br><br>2008-SEP-02 2008-OCT-15 (34291 KSK)<br><br>2008-SEP-24 2008-SEP-30 (46716 ZSK) | 2007-JAN-01 2008-DEC-31 (04183 KSK)<br><br>2008-JAN-01 2009-DEC-31 (34291 KSK)<br><br>2008-SEP-01 2008-OCT-15 (46716 ZSK) | -----BEGIN PGP SIGNED MESSAGE-----<br>Hash: SHA1<br><br>$ORIGIN .<br>@ 1 IN DNSKEY 257 3 5 (<br>AwEAAbWMiPoQlFp+snq84lbEPx2kPgessP9l<br>ieS+jeabIsxi9tE9MCbEeCrRqPtKTlp50l+C<br>0cvapYFAsg8VhyDIMlTpyw8KHTgh267GciKf<br>VkxRRZy68ndKRHC/bq8zqD4cYxVdJofTbIAm<br>bxdX80dYwtJ7ZFS7Bl4aSSQ/ly/8stX+l3oA<br>PgSbcIhjCMKzH0loR9npD6gGJpUud5zoyGl+<br>GkVvuD7XPQpzmq08KAyMz7/Nh2MmJHzfWp4L<br>glqT4cdCT/S8YTdE46I9+vDGlhknHIyEyI5m<br>P9kZWXZa58wWbv9ZBTzNOPNPWQHfPWp045wU<br>AqrRagTbRs7sWw/fpKgC5I0=<br>) ; key id = 4183<br>1 IN DNSKEY 257 3 5 (<br>AwEAAff8EiNa/S3wovNzPUmuBqelpSjnNoen<br>cXDNMpmjTgngGMPct+8KDKxM6FwvPSRxl5gN<br>RyRQfzSPU0WshDNkBV2TMtVpzqn/dsurbmTo<br>ixRzLyLK2Kd2adg5o5yS/gaTgCo0HVBmIruS<br>N3FVI2ugCWJBFLkFGHLvMJ0BTSYVqWGwQIzp<br>EPKCbKN+L9nrLcvJRCWG59Yq6BUsSEKlzSK3<br>jMhYQs6y5IiCGAVol+3VyjN93/lXkeUG6u7d<br>lQsyiY9fxfeUvmn004y0TjAgjZqdwKZB0K9M<br>A7qcALG3Tw2TXEdQsn9aY3DzNii3YEBidzER<br>mY7n4hIUrilr59MnuNJq2x0=<br>) ; key id = 34291 |

Wasn’t done alone: Thanks to: Paf, Olaf, Roy, Jakob, Dickinson, Russ, Soltero (.pr), Crocker, drc, Don Davis, David Miller, …

Thank you for listening

Questions ?