DNSSEC @ IANA

2007 ICANN Meeting Los Angeles
DNSSEC Workshop

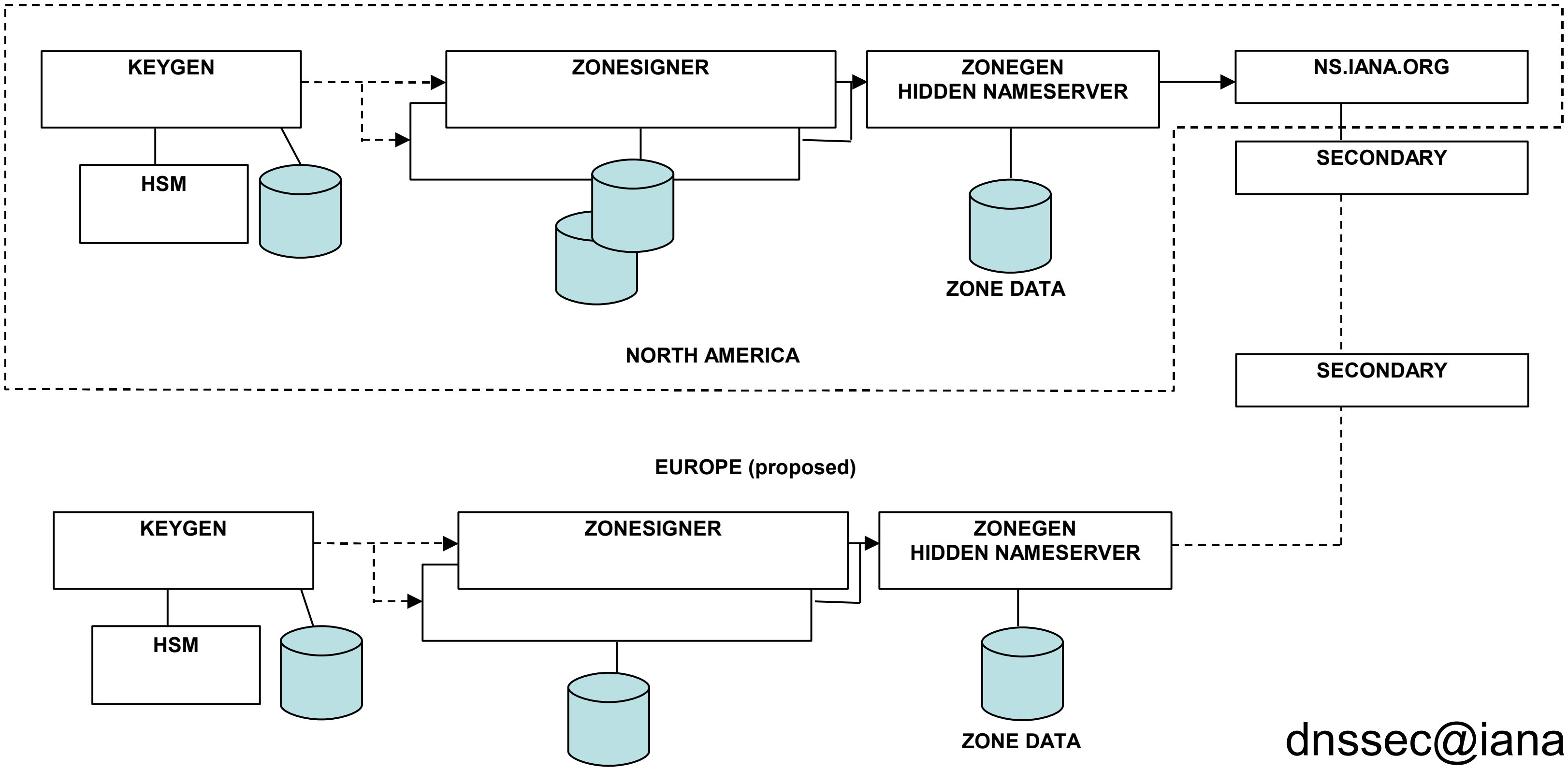
Thanks to Many!!

- IANA's design is built on the trailblazing work by .SE. Without the generous help from Jakob Schlyter and others at .SE, I would still be lost.
- Thanks to nlnetlabs.nl, Olaf, and others for the INVALUABLE “DNSSEC HowTo” and RFC4641 (DNSSEC Operational Practices) documents...
- ...and to Steve Crocker's dnssec-deployment.org initiative and the President's IANA Consultation Committee for crucial guidance.

Design Goals

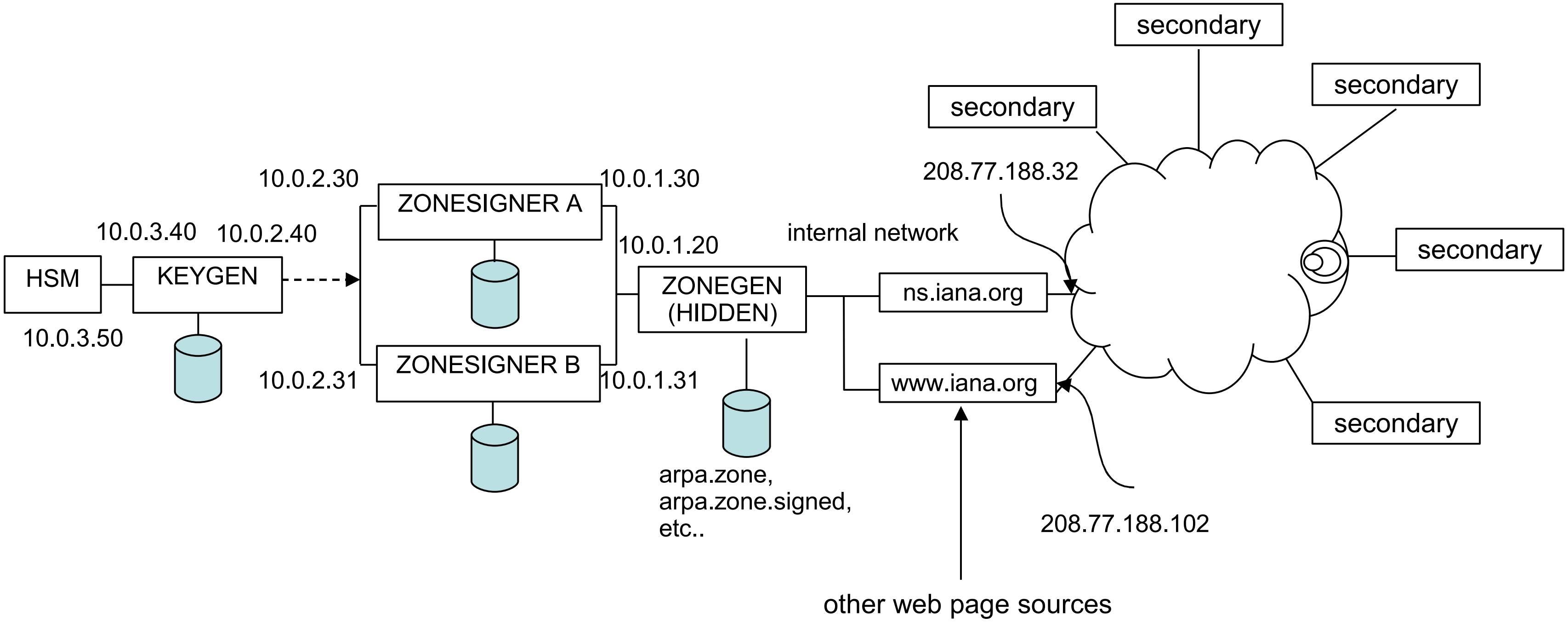
- Maintainability – if its not easy, it will fail
- Reliability – if there is a problem, no one will use it
- Security – it must look and be secure for people to trust it
- Target – arpa, in-addr.arpa, uri.arpa, urn.arpa, iris.arpa, ip6.arpa, int

“Figure 1”



dnssec@iana

Figure 1 Details



Hardware (per site)

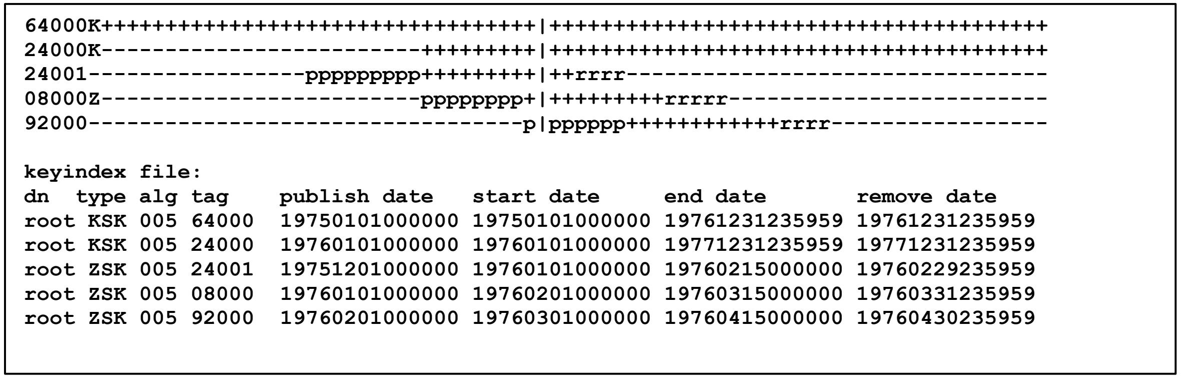
- 4x Dell 1RU 1950 commodity servers
- 1x AEP Keyper Pro (FIPS 140-2 Level 4) external Hardware Security Module (HSM)
- 1x KVM console
- Smart cards, Flash drive
- Locked rack within ICANN cage at secure colo facility

Maintainability - Only Two Scripts

- On ZONESIGNER – **signall**: 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.
- On KEYGEN – **keyall**: manually run monthly (when notified by email). Generates new keys and signed key bundles for ZONESIGNERs as needed. Also backs up any new 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 generation and rollover automated in **keyall**



```
64000K++++++++++++++++++++++++++++++++++|+++++++++++++++++++++++++++++++++++++++
24000K-------------------------+++++++++|+++++++++++++++++++++++++++++++++++++++
24001-----------------ppppppppp+++++++++|++rrrr---------------------------------
08000Z-------------------------pppppppp+|+++++++++rrrrr-------------------------
92000----------------------------------p|pppppp++++++++++++rrrr-----------------

keyindex file:
dn   type alg tag    publish date   start date     end date       remove date
root KSK 005 64000  19750101000000 19750101000000 19761231235959 19761231235959
root KSK 005 24000  19760101000000 19760101000000 19771231235959 19771231235959
root ZSK 005 24001  19751201000000 19760101000000 19760215000000 19760229235959
root ZSK 005 08000  19760101000000 19760201000000 19760315000000 19760331235959
root ZSK 005 92000  19760201000000 19760301000000 19760415000000 19760430235959
```

Maintainability – Compromised Key, Replacement Script

- For bad ZSK (old, active, new keys)
  - old – replace key with newly generated “old” key.
  - active – use old key to sign and generate a replacement. Phase out bad key.
  - new – replace key with newly generated “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 newly generated KSK with the same effectivity period and immediately publish.
  - Both – generate two keys and phase out bad keys?
- Process semi-automated with **badkey** script

Reliability – Dual Signers

- Signatures on zone records are only valid for six (6) days to limit replay attacks. So an inability to sign for more than 6 days will result in DNSSEC validation to fail.
- Design: Two (2) commodity hardware based ZONESIGNERs periodically executing **signall** to make sure the zone gets signed by one of them.

Reliability - Key Backup

- Must backup even private keys to recover from catastrophe

- Encrypt and propagate new private key material as key operations generate them

- Built into regular key operations script **keyall**

Security – KSK/ZSK Split

- Following .SE’s lead, sensitive KSK operations are kept separate from routine ZSK signing operations by only exporting pre-signed public key bundles and a single private ZSK from KEYGEN to ZONESIGNERs.

- KEYGEN machine is connected to ZONESIGNERs only during key generation and transfer operations

Security – HSM

- To protect against internal as well as external attacks, KSK operations (generation, signing, backup) for critical zones are performed inside the HSM.
- Do this using modified BIND tools with native PKCS11 support
- To minimize HSM operational overhead, child zones falling under .arpa will not use the HSM for KSK operations. Recovery from child zone KSK compromise can be effected quickly

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

Security – Key Backup

- Keys generated inside HSM (KSKs) are encrypted inside HSM before export
- Unencrypted key material (e.g. ZSK), key index, encrypted HSM keys (above), HSM configuration, and any other updated material on KEYGEN’s hard drive is further encrypted using internal HSM key before transmission/backup
- Only another HSM with the same internal HSM key can decrypt this material
- Internal HSM key backed up on N of M smartcards

Security - Meatspace

- Key generation operation requires:
  - Access to DNSSEC equipment at a secured colo facility
  - One Security Officer smartcard and PIN to enable the HSM
  - HSM User PIN to generate keys and sign the key bundle
- A minimum of two (2) authorized personnel, controlling different components above, must be present for the entire key generation operation.
- Every access to DNSSEC equipment is logged in a DNSSEC log book
- **keyall** propagates its activities to the DNSSEC Administator via email
- Material used to (re)build KEYGEN and HSM contents will be stored in safety deposit boxes. Each box will contain one of the required 2 out of 4 HSM master key smartcards along with an encrypted backup of current KSKs and miscellaneous configuration files needed for rebuilding

Software

All software and modifications will be available as open source

KEYGEN

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

ZONESIGNER

- signall, zsign, and support programs

ZONEGEN

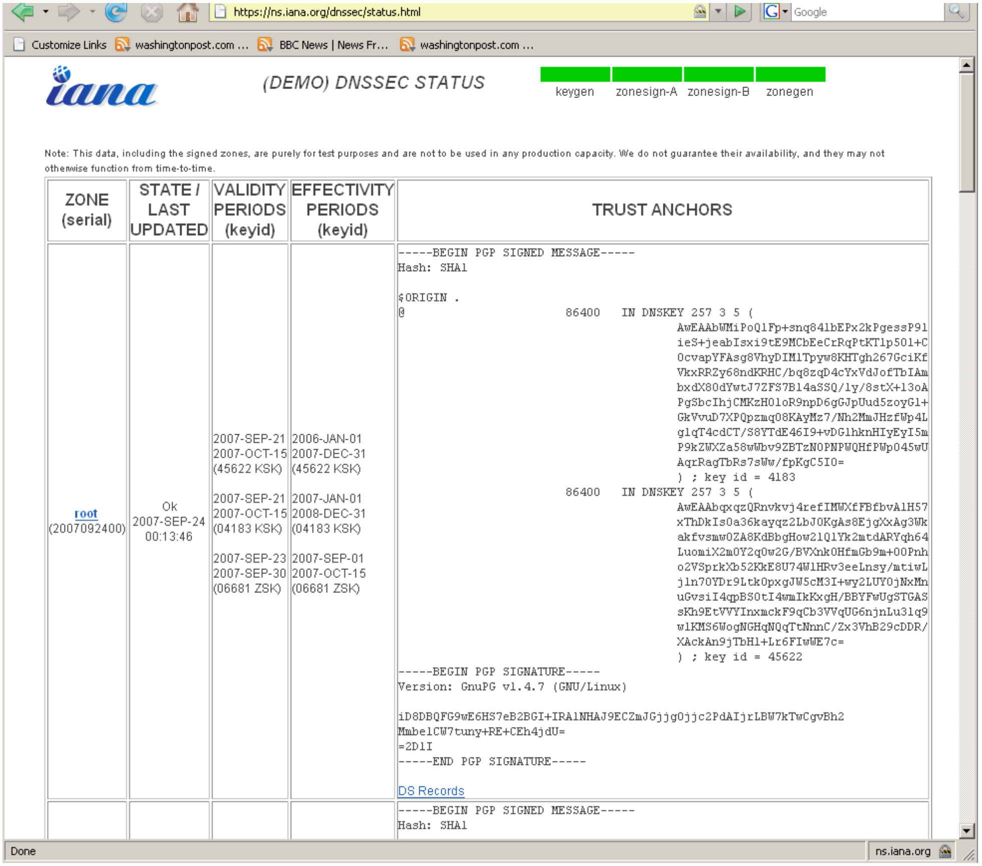
- upsite – DNSSEC status web page generator

DNSEC Status Page

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

System status and publication of PGP signed trust anchors only on SSL secured site.

Domains: root, arpa, in-addr.arpa, uri.arpa, urn.arpa, iris.arpa, ip6.arpa, int



(DEMO) DNSSEC STATUS

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>
<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>
<tr><td>root
(2007092400)</td><td>Ok
2007-SEP-24
00:13:46</td><td>2007-SEP-21
2007-OCT-15
(45622 KSK)

2007-SEP-21
2007-OCT-15
(04183 KSK)

2007-SEP-23
2007-SEP-30
(06681 ZSK)</td><td>2006-JAN-01
2007-DEC-31
(45622 KSK)

2007-JAN-01
2008-DEC-31
(04183 KSK)

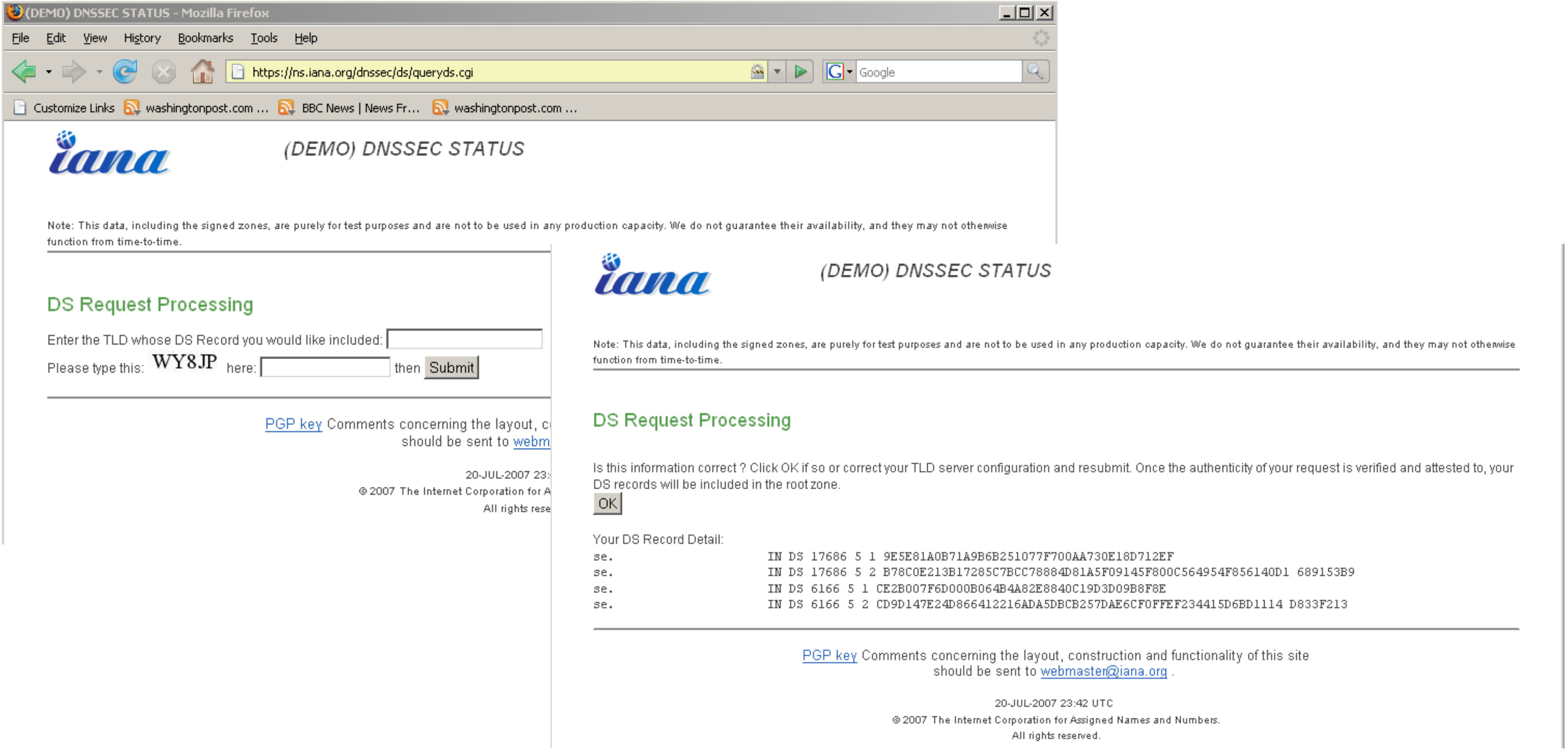
2007-SEP-01
2007-OCT-15
(06681 ZSK)</td><td><pre>
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

$ORIGIN .
@   86400   IN DNSKEY 257 3 5 (
                                        AwEAAbWMiPoQ1Fp+snq84lbEPx2kPgessP9l
                                        ieS+jeabIsxi9tE9MCbEeCrRqPtKTlp50l+C
                                        OcvapYFAsg8VhyDIMlTpyw8KHTgh267GciKf
                                        VkxRRZy68ndKRHC/bq8zqD4cYxVdJofTbIAm
                                        bxdX80dYwtJ7ZFS7Bl4aSSQ/ly/8stX+l3oA
                                        PgSbcIhjCMKzH0loR9npD6gGJpUud5zoyGl+
                                        GkVvuD7XPQpzmq08KAyMz7/Nh2MmJHzfWp4L
                                        glqT4cdCT/S8YTdE46I9+vDGlhknHIyEyI5m
                                        P9kZWXZa58wWbv9ZBTzN0PNPWQHfPWp045wU
                                        AqrRagTbRs7sWw/fpKgC5I0=
) ; key id = 4183
                        86400   IN DNSKEY 257 3 5 (
                                        AwEAAbqxqzQRnvkvj4refIMWXfFBfbvAlH57
                                        xThDkIs0a36kayqz2LbJ0KgAs8EjgXxAg3Wk
                                        akfvsmw0ZA8KdBbgHow2lQlYk2mtdARYqh64
                                        LuomiX2m0Y2q0w2G/BVXnk0HfmGb9m+00Pnh
                                        o2VSprkXb52KkE8U74WlHRv3eeLnsy/mtiwL
                                        jln70YDr9Ltk0pxgJW5cM3I+wy2LUY0jNxMn
                                        uGvsiI4qpBS0tI4wmIkKxgH/BBYFwUgSTGAS
                                        sKh9EtVVYInxmckF9qCb3VVqUG6njnLu3lq9
                                        wlKMS6WogNGHqNQqTtNnnC/Zx3VhB29cDDR/
                                        XAckAn9jTbHl+Lr6FIwWE7c=
) ; key id = 45622
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.7 (GNU/Linux)

iD8DBQFG9wE6HS7eB2BGI+IRAlNHAJ9ECZmJGjjg0jjc2PdAIjrLBW7kTwCgvBh2
MmbelCW7tuny+RE+CEh4jdU=
=2DlI
-----END PGP SIGNATURE-----
</pre>DS Records</td></tr>
<tr><td></td><td></td><td></td><td></td><td><pre>
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
</pre></td></tr>
</table>

DS Record Handling

- Integrate into IANA root zone management?
- https://ns.iana.org/dnssec/ds/queryds.cgi



(DEMO) DNSSEC STATUS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://ns.iana.org/dnssec/ds/queryds.cgi
Google
Customize Links
washingtonpost.com ...
BBC News | News Fr...
washingtonpost.com ...
iana

(DEMO) DNSSEC STATUS

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.

DS Request Processing

Enter the TLD whose DS Record you would like included:

Please type this: WY8JP here: then Submit

PGP key Comments concerning the layout, c
should be sent to webm

20-JUL-2007 23:

© 2007 The Internet Corporation for A

All rights rese

(DEMO) DNSSEC STATUS

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.

DS Request Processing

Is this information correct ? Click OK if so or correct your TLD server configuration and resubmit. Once the authenticity of your request is verified and attested to, your DS records will be included in the root zone.

OK

Your DS Record Detail:

```
se.                     IN DS 17686 5 1 9E5E81A0B71A9B6B251077F700AA730E18D712EF
se.                     IN DS 17686 5 2 B78C0E213B17285C7BCC78884D81A5F09145F800C564954F856140D1 689153B9
se.                     IN DS 6166 5 1 CE2B007F6D000B064B4A82E8840C19D3D09B8F8E
se.                     IN DS 6166 5 2 CD9D147E24D866412216ADA5DBCB257DAE6CF0FFEF234415D6BD1114 D833F213
```

PGP key Comments concerning the layout, construction and functionality of this site
should be sent to webmaster@iana.org .

20-JUL-2007 23:42 UTC

© 2007 The Internet Corporation for Assigned Names and Numbers.

All rights reserved.

Questions I have

- How’s it look?
- Compromised key recovery in the face of disinterested users. Update vectors:
  - Windows update, anti-virus software updates, RFC5011/Revoke bit St. Johns,..?
- How to detect compromised keys?
- Other DS record acceptance/derivation mechanisms?
- Other suggestions?