

# Signing of the Root Zone

Gaurab Raj Upadhaya  
[gaurab@lahai.com](mailto:gaurab@lahai.com)

<http://www.gaurab.org.np/?p=27>

# DNSSEC 101

- Cryptographic signing of the DNS data, so that the recipient can verify the integrity of the data
- Key Signing Key signs the Zone Signing Key which then signs the actual zone.
- Almost 15 years old Protocol, major traction in the last 3 years

# Significance of the Root Key Signing

- The 'DNS Root' lies at the top of the DNS hierarchy.
- It's probably the most natural trust anchor for signing of the DNS tree (*not all people agree*).
- A path for deployment of DNSSEC more widely, as people no longer can claim that the hierarchy is incomplete

# Signing Operations

- ICANN DNS Ops : <http://dns.icann.org>
- Root DNSSec: <http://www.root-dnssec.org/>
- KSK and ZSK split operations
  - ICANN does the KSK
  - Verisign does the ZSK
- Trusted Community Representatives (TCRs)

# June 16, 2010

- First Key Signing Ceremony in Culpeper, VA
- What happened ?
  - Hardware Security Module (HSM) initialized
  - Seven Crypto Officers (CO) incorporated - \*(I am one of them)
  - Seven Recovery Key Share Holders (RKSH) incorporated
  - Generate the KSK
    - Received the Key Signing Request from Verisign, containing the ZSK - signed them and returned the Signed Key Response, which will be used to sign the root zone by Verisign.
- A major Milestone

# Signed Zone

- Second Key Signing Ceremony on 12th July in El Segundo, CA
- Similar process as before, but no new key generated (same key as previously generated used)
- On 15th July, the root servers started serving the signed DNS Root Zone.



```
Starting: kskgen (at Wed Jun 16 21:19:06 2010 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
  Label:          ICANNKSK
  ManufacturerID: AEP Networks
  Model:          Keyper Pro 0405
  Serial:         K6002013
```

```
Generating 2048 bit RSA keypair...
Created keypair labeled "Kjqmt7v"
```

```
SHA256 DS resource record and hash:
. IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5
>> deckhand pedigree snapline breakaway kickoff hemisphere flytrap detergent guidance c
oherence eating outfielder facial hurricane hamlet fortitude keyboard Bradbury cranky l
eprosy Dupont adroitness willow Chicago tempest sandalwood tactics component uproot dis
tortion payday positive <<
```

```
Created CSR file "Kjqmt7v.csr":
O: ICANN
OU: IANA
CN: Root Zone KSK 2010-06-16T21:19:24+00:00
1.3.6.1.4.1.1000.53: . IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2C
E1CDDE32F24E8FB5
```

```
Kjqmt7v.csr SHA256 thumbprint and hash:
401120C1721BA100B2D9ABF2D01332399535BA0F9C71DBD9F97232C5EBD608D2
>> crackdown Babylon bison recover highchair bravado ratchet adroitness sawdust support
ive rhythm vagabond stagnate barbecue checkup corporate preclude conformist shadow atmo
sphere python hideaway suspense supportive waffle holiness checkup resistor trouble spe
culate aimless sensation <<
```

```
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```

```
Applications Places System
root@localhost:~#
keyboard Bradbury cranky leprosy Dupont adroitness willow Chicago tempest
sandalwood tactics component uproot distortion payday positive <<
Created CSR file "Kjqmt7v.csr":
O: ICANN
OU: IANA
CN: Root Zone KSK 2010-06-16T21:19:24+00:00
1.3.6.1.4.1.1000.53: . IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1
A41855200FD2CE1CDDE32F24E8FB5
Kjqmt7v.csr SHA256 thumbprint and hash:
401120C1721BA100B2D9ABF2001332399535BA0F9C71DBD9F97232C5EBD608D2
>> crackdown Babylon bison recover highchair bravado ratchet adroitness so
wdust supportive rhythm vagabond stagnate barbecue checkup corporate precl
ude conformist shadow atmosphere python hideaway suspense supportive waffl
e holiness checkup resistor trouble speculate aimless sensation <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
***** Log output in ./kskgen-20100616-211906.log *****
[root@localhost HSMFD]#
```





# More info

- <https://www.iana.org/dnssec/>
- Various Tutorials at APNICs, APRICOTs, SANOGs.....

**Thank you**