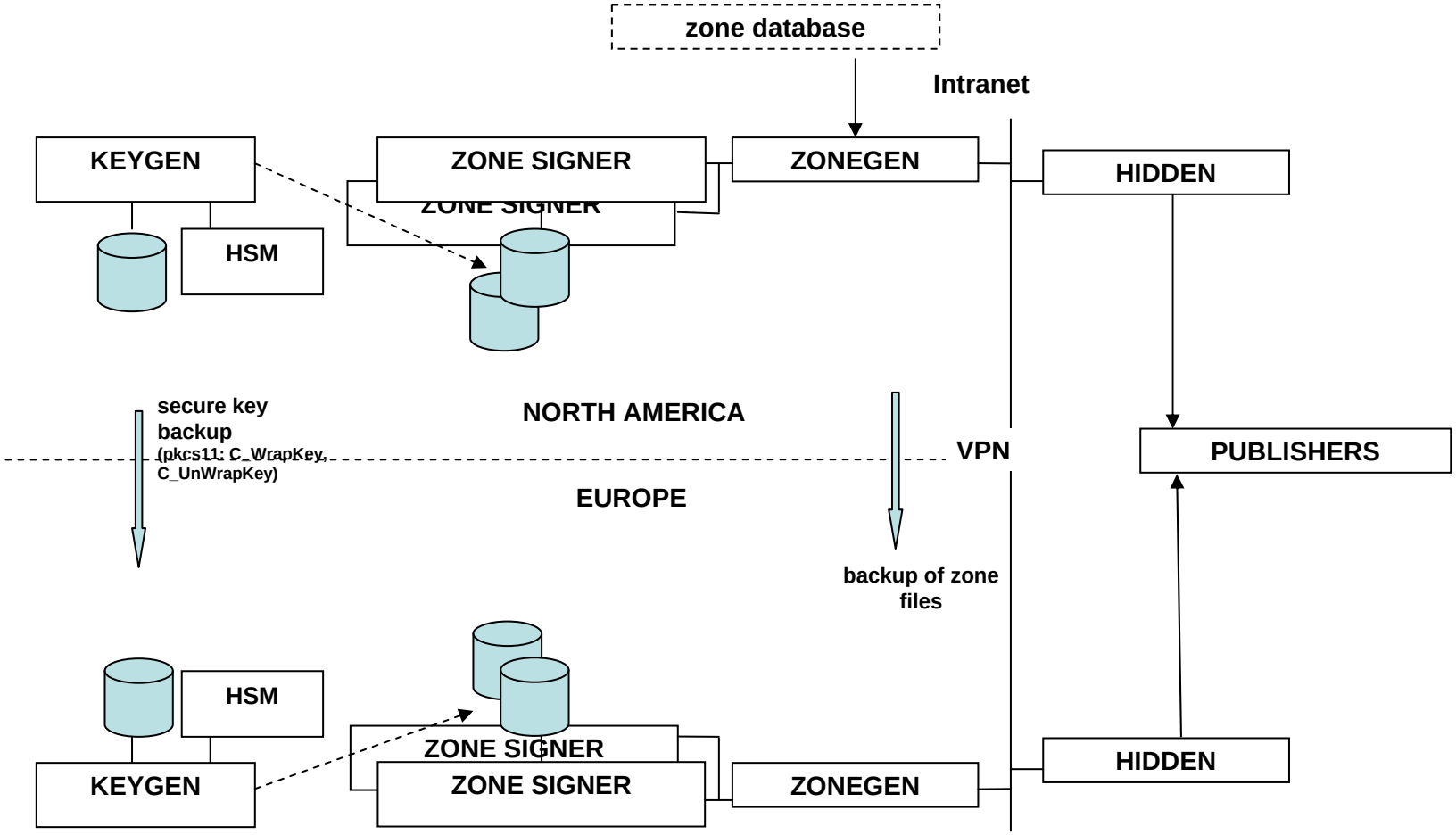
DNSSEC @ IANA

“Figure 1”


zone database
Intranet
KEYGEN
ZONE SIGNER
ZONEGEN
HIDDEN
HSM
ZONE SIGNER
secure key backup
(pkcs11: C_WrapKey, C_UnWrapKey)
NORTH AMERICA
VPN
PUBLISHERS
EUROPE
backup of zone files
HSM
ZONE SIGNER
KEYGEN
ZONE SIGNER
ZONEGEN
HIDDEN

Two Central Functions

- zonesigner – **signall**: automatically run daily on multiple machines to pickup zone changes (based on SOA serial) or freshen signatures, reload zonegen, check key status, update web page, email notifications.
- keygen – **keyall**: manually run monthly (or when notified by zsign) script to generate new keys and sign keybundles.
- Misc/support
  - zonesigner - upsite: create status web page
  - zonegen - idlenot: system health checks
  - keygen - keybackup: extract encrypted key blobs from HSM and propagate to backup site
  - bind dnssec tools, ntpd

Normal key rollover

- Based on .se design. Multiple overlapping keys (effectivity periods)
- ZSK - three (3) overlapping ZSKs /w staggered effectivity periods. Only one signs records
- KSK - two (2) overlapping KSKs /w staggered effectivity periods. Both sign the “key bundle” of five (5) keys
- Process built into kgen script

```
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
```

Emergency key rollover

- ZSK
  - Old – replace key with newly generated “old” key.
  - Active – use new or old key to sign and generate a replacement. Phase out bad key.
  - New – replace key with newly generated “new” key.
  - DNS propagation delay: Two-phase process when “close” to a transition otherwise publish immediately.
- KSK
  - One - replaced key with newly generated KSK with the same effectivity period and immediately publish.
  - Both – generate two keys and phase out bad keys.
- Process built into kgen script

Hardware at each site

- 4x Dell 1RU 1950 server
- 1x AEP Keyper Pro (FIPS 140-2 Level 4) external HSM
- 1x KVM console
- Smart cards, Flash drive
- Locked rack within ICANN cage as secure colo

DNSEC Status Page

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

Domains: root, arpa,
uri.arpa, urn.arpa,
iris.arpa, ip6.arpa, int

Questions I have

- Hows it look?
- Compromised key recovery in the face of lackadaisical users
  - Windows update, anti-virus updates, takrem, St. Johns,..?
- Simplify HSM/keygen setup ?
- How to detect compromised keys?
- Other suggestions?