DNSSEC zone-signing tool chest

UKUUG Spring 2011 Conference
Leeds, UK
March 2011

Jan-Piet Mens

```
$ dig 1.1.0.3.3.0.8.1.7.1.9.4.e164.arpa naptr
```

DNS used to be easy

- Set up a name server. Any name server.
- Add a zone or two

```
@        3600 IN SOA u.six53.net. noc.six53.net. (
                    1 86400 10800 3600000 3600 )
        86400 IN NS c.six53.net.
        86400 IN NS a.six53.net.
         3600 IN MX 10 mail.jpmens.org.
www      3600 IN A  10.0.1.2
mail     3600 IN A  10.0.1.3
```

- Done
- If it worked, it worked for ever and a day

DNS has become a wee more complex

- Set up a server which supports DNSSEC
- Create a zone (or two)
- Create private and public keys
- Sign the zone
- Go to previous step

Keys

- Typically a zone will be signed by two or more keys
- KSK
  - Key-Signing Key
- ZSK
  - Zone-Signing Key
- Algorithms
  - Lots to choose from: RSAMD5, DSA, ECC, RSASHA1, RSASHA1-NSEC3, RSASHA256, ECC-GOST, ...

Signatures

- RRSIGs
  - Have inception and expiration dates
    - Fixed timestamp in UTC, not relative period like TTL
  - Must be renewed before expiration date expires!
    - Monitoring

`https://github.com/dotse/dnssec-monitor`

Authenticated denial of existence

- NSEC
  - Proves non-existence using signed record that indicates nothing between "ldap" and "mail".
  - NSEC data generated for the whole zone
  - Zone becomes "walkable". (Privacy policy?)
- NSEC3 opt-in
  - Proves non-existence using signed record that indicates nothing is between H("ldap") and H("mail") in hash order.
  - NSEC3 opt-in data is generated for the whole zone
- NSEC3 opt-out
  - Same as opt-in, but NSEC3 opt-out is not generted for whole zone but only for authoritative data and for delegation to signed zones.
    - e.g. .FR has around 4M records but only handful of signatures

Open-Source Signers

- BIND smart-signing
- BIND auto-sign
- ZKT
- OpenDNSSEC
- PowerDNS (>= 3.0)
- Other

BIND utilities: create keys

- Generate a ZSK and a KSK

```
$ dnssec-keygen -a RSASHA256 -b 1024 jpmens.org
Generating key pair..
Kjpmens.org.+008+56445

$ dnssec-keygen -a RSASHA256 -b 1024 -f ksk jpmens.org
Generating key pair..
Kjpmens.org.+008+61999
```

- The .key files contain the public key (i.e. the DNSKEY record). Keep .private files safe

```
$ ls -1 K*
Kjpmens.org.+008+56445.key
Kjpmens.org.+008+56445.private
Kjpmens.org.+008+61999.key
Kjpmens.org.+008+61999.private
```

BIND utilities: sign zone

- Sign zone: smart signing

```
$ dnssec-signzone -S -o jpmens.org zone.db
Fetching ZSK 56445/RSASHA256 from key repository.
Fetching KSK 61999/RSASHA256 from key repository.
Verifying zone using following algorithms: RSASHA256.
Zone signing complete:
Algorithm: RSASHA256: KSKs: 1 act, 0 stand-by 0 revoked
                      ZSKs: 1 act, 0 stand-by 0 revoked
zone.db.signed
```

- Signed

```
$ wc zone.db*
  6   36  242 zone.db
101  293 3982 zone.db.signed
```

Zone file: after signing

```
; File written on Thu Mar 10 19:55:03 2011
; dnssec_signzone version 9.8.0
jpmens.org.         3600  IN SOA u.six53.net. noc.six53.net. (
                                 1          ; serial
                                 86400      ; refresh (1 day)
                                 10800      ; retry (3 hours)
                                 3600000    ; expire (5 weeks 6 days 16 hours)
                                 3600       ; minimum (1 hour)
                                 )
                    3600  RRSIG  SOA 8 2 3600 20110409175503 (
                                 20110310175503 56445 jpmens.org.
                                 VwdXlhiIONzBZKE2/JUDVJsTNNGXegUs04YH
                                 k1BVXEsQvdhzykK+5fItvz4g7Za9TXKEdKQr
                                 x0xsmrPqv16/Cd8ZwlZv97WYGaMBclH55xCE
                                 5Xd6LMmNoXLPPqSPIz1nOP0YKpbdWVKGwxYk
                                 +VHakcGVcWwxMo5DLmrF7ha7GHw= )
                    86400 NS     a.six53.net.
                    86400 NS     c.six53.net.
                    86400 RRSIG  NS 8 2 86400 20110409175503 (
                                 20110310175503 56445 jpmens.org.
                                 s7M++oU+EM3LjRxrQsEU3KydhtPKavHqTVwW
                                 LQjUepv2YWqFzu/tJ4K7GV5j/Cu1ceY0NKq2
                                 SLWW6VvCyoyQCwJMMw50BAAqLloa5JQ1vBti
                                 nUEPB5zvB8L3s9Y0kCXGhu445Ppzb66zSijV
                                 pIX0dJGNcFUPNIWwhkbN84y3uMw= )
                    3600  MX     10 mail.jpmens.org.
                    3600  RRSIG  MX 8 2 3600 20110409175503 (
                                 20110310175503 56445 jpmens.org.
                                 l4YR2DFMIrcHkULGaxXlgz6kRITVl8NrvALG
                                 swkeiXXbeI7jUKp7sFSh/ER61OrnSMvBNj1e
                                 sGt5NHbab8hGBV2smL5WLQX96Ornz/aqkioY
                                 utLLcx5KWih0m85CGoim3Jmb+T+ta/uhRrA+
                                 XJj2PwyNIX4R/RcdHLmzcIzUpjc= )
                    3600  NSEC   mail.jpmens.org. NS SOA MX RRSIG NSEC DNSKEY
                    3600  RRSIG  NSEC 8 2 3600 20110409175503 (
                                 20110310175503 56445 jpmens.org.
                                 lizidOqWl6ZYnqmGZubvGvRsSz7EWc9Xs6eu
                                 wXGfLZk5xkuJrVFbxQBNF4m3woLoi+ElQWiY
                                 1GTMfFwJFPQLCooIPLPrXUK58CS92x9g4ADo
                                 /uxdslMgGxUOjFvtlzGIXINCHXhYEc34LZ+H
                                 uxSMVUXZ2v16oHwCN6RN5PKPfJY= )
                    3600  DNSKEY 256 3 8 (
                                 AwEAAdXfM5Mwwaa8U+z0R6mB/BAGAjb6Vt0v
                                 /CFJjltI+joiPLf+5MkCIqBnYlnG0s+qWQ4e
                                 t9etcbew6RZgBSJ2BqlZllflXpLfCGmEqvx6
                                 /La+86AsoJyOgXfU2OgDLeH6bg9+kMVqZmv7
                                 CwXjbvWzHzGu/43EEn5gqvqgX1prlsT7
                                 ) ; key id = 56445
                    3600  DNSKEY 257 3 8 (
                                 AwEAAdTEIlEAkL945VeP1ePXOt5k0gbD6UzH
                                 LjmP45CWxmH5EthWh1MkFgmrLAAXFpfv6Lz3
                                 8wluI0o+7qgAuW+g8MJUV2pYPj7J6apHoeKX
                                 AhyJ9Tgf2qOu9GTsK+6qy3A7+e/aUX1iYmNS
                                 6wbWiRAiWv25D74PUrM+uoDC0Vk5hxPV
                                 ) ; key id = 61999
                    3600  RRSIG  DNSKEY 8 2 3600 20110409175503 (
                                 20110310175503 56445 jpmens.org.
                                 BWdhA+Ln6uAhHZHlDxis3N9E+9cwiyYP76Lc
                                 GL/l0f9CcK0ObEt9uwR0LLBkW0BwxadbVPh0
                                 zbMFSd8OkSBO//eKM6ApowTM8ZB/gdnTk/5L
                                 S/KuU8+nsrU9Yzr38JUUil40m3zFmWrYhalJ
                                 LeQxReByB/UeTbSKDn11R6P/sFQ= )
                    3600  RRSIG  DNSKEY 8 2 3600 20110409175503 (
                                 20110310175503 61999 jpmens.org.
                                 wXKcBmU+GVi9P+r0zGOjlL+iaHRjDicIjeas
                                 lYy0apLa+0hTaoqLXpO6IER9VqgDmR0cRIU2
                                 lIbPt+p0OqN5pbnN6Cs+0JKhQn0K48l0C/ct
                                 8X0+Ai2mP8QJ+PcdASV0RLZmNN+bzYWrSrgC
                                 uz866nEbjJjROD2Sx9dy2Fv3atE= )
mail.jpmens.org.    3600  IN A   10.0.1.3
                    3600  RRSIG  A 8 3 3600 20110409175503 (
                                 20110310175503 56445 jpmens.org.
                                 QyGykPNX3mBamrn+2c5ab3wbVe1Qj2Rk7Uzz
                                 iOAn52Atc/uK/QyccAbL6+vSH4Sx4H62CPcM
                                 xlUh+zYNL4Tm0+D5HndFCYznu2D58/a4HXCC
                                 otcU/uZE/gsyhpwe+f5w8PRprlsP1vkUaUph
                                 jgnw+huIqQFZA4nrTbcNvp8BfnI= )
                    3600  NSEC   www.jpmens.org. A RRSIG NSEC
                    3600  RRSIG  NSEC 8 3 3600 20110409175503 (
                                 20110310175503 56445 jpmens.org.
                                 bnvRKz6zCMZnhfDUu0xQw6yuDupXKLqFOJgQ
                                 1balmzQsMRzhZeF2jjdeu2xy/gUmi9WUJZzx
                                 gyyiD8G6layLZRWZkGLhIEL7c9LpwlQI5QeX
                                 T6P/+6xllpipxgX8QKwHrhxFBlv5xsHg2sa0
                                 RCZJ4JHsXdtbYy6M95bV+L1a8Qc= )
www.jpmens.org.           3600  IN A   10.0.1.2
                    3600  RRSIG  A 8 3 3600 20110409175503 (
                                 20110310175503 56445 jpmens.org.
                                 BTTZQrNXEhdCylJ1ouWdix3WnbAaXCgIvkA0
                                 NYcNvkqN5sLHohoVC0EUJ0Q55g0Yx+9bo3jc
```

BIND utilities: sign zone (2)

- dnssec-signzone also creates DS set for submission to parent zone

```
jpmens.org. IN DS 61999 8 1 DC2FB...525E0
jpmens.org. IN DS 61999 8 2 1DA...78A5D1E8
```

- Parent zone needs DS record(s)
- Some registrars expect DNSKEY from which they compute DS
- Submission is "difficult"

BIND: configure server

- BIND has to be told to serve DNSSEC-signed zones

```
options {
  dnssec-enable yes;
};

zone "jpmens.org" in {
  type "master";
  file "zone.db.signed";
};
```

- NSD serves DNSSEC-signed zones without special configuration

BIND auto-sign

- Since BIND 9.7
- Key files include meta data as comments, used by BIND

```
$ head -4 Kjpmens.org.+008+61999.key
; This is a key-signing key, keyid 61999, jpmens.org.
; Created: 20110310184842 (Thu Mar 10 19:48:42 2011)
; Publish: 20110310184842 (Thu Mar 10 19:48:42 2011)
; Activate: 20110310184842 (Thu Mar 10 19:48:42 2011)
```

- Utility dnssec-settime modifies that meta data
- BIND uses embedded meta data as key policy during smart-signing (-S) and auto-signing

BIND auto-sign (cont'd)

- Automatic zone signing (BIND >= 9.7)

```
zone "jpmens.org" in {
   type master;
   key-directory "keys";
   update-policy local;
   auto-dnssec maintain;
   sig-validity-interval 30;  // days
   file "jpmens.org";
};
```

- BIND daemon (named) automatically signs zone
- "maintain" means sign as new records are updated (RFC 2136)
- If keys are available in key-directory, adding DNSKEY records, performs key rollover

ZKT: Zone Key Tool

- Created by Holger Zuleger http://www.hznet.de/dns/zkt/ in BIND contrib/
- Wrapper around dnssec-keygen and dnssec-signzone
- Policy file per zone / per directory

```
/zones
   - dnssec.conf
   - net/
       example.net/
          - zone.db
- zone.db.signed
```

- Automates key generation and zone signing
- Ideal for cron(8)

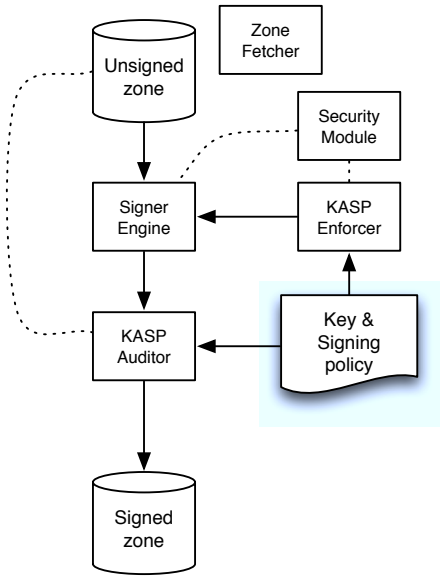
```
zkt-signer -D . -v
```

- Can work recursively over directory tree

OpenDNSSEC

- Created as a "turn-key solution"
- Supports HSM & provides SoftHSM (PKCS#11)
- Automatic key management
- Database support (SQLite3 & MySQL)
- Large dependency list (Ruby, ldns, libxml, Ruby Gems, db, Botan)
- Configuration in XML files, copied to database
- Supports NOTIFY/AXFR to signing engine; script invoked when zone signed
- Performance & concurrency are issues with many zones
- Complex

OpenDNSSEC Architecture



OpenDNSSEC

- Notifications
  - DNS NOTIFY to zonefetcher for incoming AXFR
  - DS notify script to submit DS to parent

PowerDNS

- PowerDNS 3.0 (almost ready for prime time)
- Supports pre-signed zones or live-signing operations
- Otherwise zone data and keys/signatures separate
- Small change in database schema
- Off we go:

```
$ pdnssec secure-zone jpmens.org
```

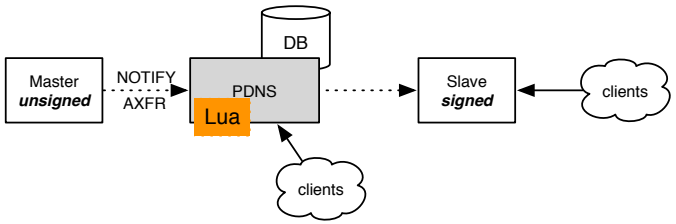
- That's it. Honest!

PowerDNS (cont'd)

- Can import existing (BIND) keys (v1.2)
- Keys are in back-end database (gmysql, gpgsql, gsqlite) and need to be protected
  - It's a bit like a private key for your HTTPS server
  - Alternatively run in pre-signed mode
  - Encrypted file system
- Supports NSEC and NSEC3
- Signatures (RRSIG records) are calculated on the fly
  - Inception: previous Thursday
  - Expiration: Thursday two weeks later
  - No issue if PDNS is authoritative, but watch out if hidden master
- No DNSSEC relevance: PDNS 3.0 also has TSIG for AXFR

PowerDNS: modes of operation

- Authoritative
- In-line signer



- Lua script on AXFR
  - Consistent SOA, NS RRset
  - Timestamp

    `http://mens.de/:/c8`

PowerDNS: pdnssec

- New utility: pdnssec

```
$ pdnssec secure-zone $z            # creates 2 keys
$ pdnssec add-zone-key $z ksk rsasha256 # adds ksk
$ pdnssec show-zone $z            # output formatted
Zone has hashed NSEC3 semantics
Zone is not presigned
keys:
ID = 7 (KSK), tag = 41120, algo = 8, bits = 2048
KSK DNSKEY = jpmens.org IN DNSKEY 257 3 8 Aw..5uc8=
DS = jpmens.org IN DS 41120 8 1 3296abd...b93
DS = jpmens.org IN DS 41120 8 2 4bb00a5...fa1b78b
DS = jpmens.org IN DS 41120 8 3 3c01686...50be3e4
ID = 8 (ZSK),tag = 50853,algo = 8,bits = 1024 Active: 1
ID = 9 (ZSK),tag = 8751,algo = 8,bits = 1024 Active: 0
```

Other tools

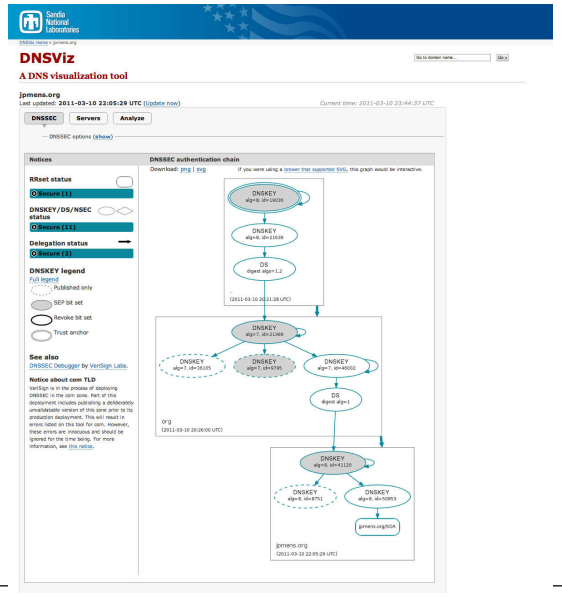
- Phreebird
  - DNSSEC proxy, automatic key generation, real-time signing. Proof of concept by @dakami

    `http://mens.de/:/9d`

Verify your zones!

- DNSViz

  `http://dnsviz.net/`



Testing & verification

- Configure island of trust in Unbound (or BIND) to test your authoritative server
- DNScheck

  `http://dnscheck.iis.se/`
- ZoneCheck

  `http://zonecheck.fr`
- DNSSEC Debugger

  `http://dnssec-debugger.verisignlabs.com/`
- YAZVS (Yet Another Zone Validation Script)

  `http://yazvs.verisignlabs.com/`
- DeNIC NAST

  `http://www.denic.de/en/background/nast.html`
- SURFnet DNSSEC monitor

  `http://www.dnssecmonitor.org/`

How to choose a signing system

- Define required level of automation
- Number and size of zones
- Required security
  - Keys on file system
  - Hardware Security Module
- Define Policies
  - Key lengths & algorithms
  - Signature lifetimes
  - Key rollovers

Lessons learned

- Always use recent software releases, even if it means building your own
- Monitor. More than you ever did
- When choosing your signing platform, throw things at it
- You need lots of random data (hw dongles)
- Get a good calendar & reminder program
- Choosing an HSM is a PITA
- DNSSEC means more data, more CPU, and more traffic. Oh, and more problems
- Did I say use recent software releases?

#FAILs

Date	TLD	Signer	Reason
20080528	NL	OpenDNSSEC	Partial zone published
20091013	SE	ODS+BIND	Corrupt zone published (not DNSSEC) [2]
20101007	BE	Homebrew	Expired signatures [4]
20100604	ARPA	?	Expired signatures [5]
20100913	UK	OpenDNSSEC	Signing failure upon failover (HSM) [3]
20100512	DE	Java	Partial zone published (not DNSSEC) [1]
20110212	FR	ODS+BIND	Invalid sigs on NSEC3 disprove DS (BIND bug)
20110215	e164	Secure64	No RRSIG on KSK [6]
20110222	KG	?	RRSIG inception times hours in future [7]

@npua: Extrapolation: If you don't hit an operational snag, DNSSEC will get you

1: http://www.denic.de/denic-im-dialog/mailinglisten/public-l.html?url=msg04454.xml
2: http://royal.pingdom.com/2009/10/13/sweden%E2%80%99s-internet-broken-by-dns-mistake/
3: http://www.nominet.org.uk/registrars/systems/serviceannouncements/?contentId=7872
4: https://lists.dns-oarc.net/pipermail/dns-operations/2010-October/006166.html
5: http://dnssec-deployment.org/pipermail/dnssec-deployment/2010-June/003881.html
6: http://dnssec-deployment.org/pipermail/dnssec-deployment/2011-March/004842.html
7: http://dnssec-deployment.org/pipermail/dnssec-deployment/2011-February/004816.html

@nerdybits

Further reading

- DNSSEC Operational Practices, version 2

  `http://tools.ietf.org/html/ \`
  `draft-ietf-dnsop-rfc4641bis-06`
- ENISA Good Practices Guide

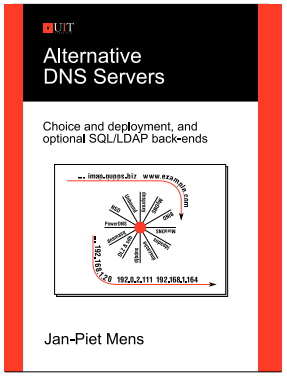
  `http://www.enisa.europa.eu/act/res/ \`
  `technologies/tech/gpgdnssec`
- NIST Secure Domain Name System (DNS) Deployment Guide

  `http://csrc.nist.gov/publications/PubsSPs.html`

Further reading

- Alternative DNS Servers, UIT, 2009, Jan-Piet Mens

  `http://mens.de/:/altdns`



Thank you

Questions?

Whoami

```
$ dig 1.1.0.3.3.0.8.1.7.1.9.4.e164.arpa naptr

;; ANSWER SECTION:
1.1.0.3.3.0.8.1.7.1.9.4.e164.arpa. 3575   IN NAPTR 3 10 "u" "E2U+http" "!^.*$!http:mens.de!" .
1.1.0.3.3.0.8.1.7.1.9.4.e164.arpa. 3575   IN NAPTR 3 20 "u" "E2U+http" "!^.*$!http:blog.fupps.com!" .
1.1.0.3.3.0.8.1.7.1.9.4.e164.arpa. 3575   IN NAPTR 4 10 "u" "E2U+mailto" "!^.*$!mailto:jp@mens.de!" .
1.1.0.3.3.0.8.1.7.1.9.4.e164.arpa. 3575   IN NAPTR 1 10 "u" "E2U+sip" "!^.*$!sip:5552064@sipgate.de!" .
1.1.0.3.3.0.8.1.7.1.9.4.e164.arpa. 3575   IN NAPTR 2 10 "u" "E2U+tel" "!^.*$!tel:+491718033011!" .
```