

# D N S S E C – Practice

## Tools

for signing and key rollover

DENIC Technical Meeting  
4. April 2006

*Holger.Zuleger@hznet.de*

## DNSsec or "How to sign a zone"

- All necessary Tools available by BIND
  - Creation of the zone key: `dnssec-keygen`
  - Signing of the zone data: `dnssec-signzone`
- No local policy definition possible
  - Algorithm
  - Key length
  - Key usage lifetime
- No automatic key rollover  
How to change the key material in the zone file?
- No automatic re-signing  
Change of the serial no?
- No zone reload

## DNSsec Practice (Bind Tools)

- Create the key material

- Key signing key (KSK)

```
$ dnssec-keygen -f KSK -n ZONE -a DSA -b 1024 example.net
```

- Zone signing key (ZSK)

```
$ dnssec-keygen -n ZONE -a RSASHA1 -b 512 example.net
```

```
$ ls -l
```

```
-rw-r--r--  1 dnsop  dnsop   581 2005-08-14 13:55 Kexample.net.+003+18710.key
-rw-----  1 dnsop  dnsop   688 2005-08-14 13:55 Kexample.net.+003+18710.private
-rw-r--r--  1 dnsop  dnsop   121 2005-08-14 13:55 Kexample.net.+005+57705.key
-rw-----  1 dnsop  dnsop   545 2005-08-14 13:55 Kexample.net.+005+57705.private
```

- Store the public part of the key in the zone file

```
$ cat Kexample.net+*.key >> zone.db
```

- Increment SOA serial number (vi?)

- Sign the zone file

```
$ dnssec-signzone -g -o example.net zone.db
zone.db.signed
```

## DNSsec Practice (2)

- Configure named

```
options {  
    dnssec-enable yes;  
};  
  
zone "example.net" {  
    type master;    file "example.net./zone.db.signed";  
};
```

- Reload the zone

```
$ rndc reload example.net
```

- Re-sign the zone before the signature times out  
But: Don't forget to increment the serial number
- Start a key rollover if the lifetime of the key is over  
There are two different ways to do this

# Key Rollover

- „DNSSEC Operational Practices“ define two algorithms for key rollover
- ZSK Rollover (pre-publish key)
  1. Generate second ZSK
  2. Publish both (public) keys, but use only the old one for signing
  3. Wait at least propagation time + TTL of the DNSKEY-RR
  4. Use new key for zone signing; leave old one published
  5. Wait at least propagation time + maximum TTL of the old zone
  6. Remove old key
- KSK Rollover (double signature)
  1. Generate new KSK
  2. Use both keys for key signing
  3. Send new DS-Record (or DNSKEY-RR) to the parent
  4. Wait until the DS is propagated + TTL of the old DS-RR
  5. Remove the old key

# DNSsec Tools

- KROd – Key Rollover Daemon ([www.idsa.prd.fr/index.php?page=kro&lang=en](http://www.idsa.prd.fr/index.php?page=kro&lang=en))
  - Full automatic ZSK rollover
  - Full automatic KSK rollover  
incl. KSK key exchange with the parent domain
  - C based wrapper around the BIND tools
  - Project is finished
- DNSSEC Key Maintenance Tools ([www.ripe.net/disi/code.html](http://www.ripe.net/disi/code.html))
  - Reference Implementation to „DNSsec Operational Practices“
  - Secure(!) private key storage (BackEnd)
  - Various front ends for key rollover and zone signing
  - Semi-automatic KSK and ZSK rollover  
(double signature & pre-publish)
  - Perl based

## DNSsec Tools (2)

- DNSsec Tools ([www.dnssec-tools.org](http://www.dnssec-tools.org))
  - Zone signing and key management tool
  - Perl based wrapper around the BIND tools
  - Includes also some resolver tools  
(Sendmail(SPF) patch, Mozilla and Thunderbird integration)
- Zone Key Tool ([www.hznet.de/zkt/](http://www.hznet.de/zkt/))
  - Automatic ZSK rollover
  - Full automatic re-signing of the zone
  - Parses secure zones out of named.conf
  - C based wrapper around the BIND tools
  - Best for small to medium domain hosting

## Zone Key Tool (ZKT)

- Provides Tools for key management and zone signing

```
$ dnssec-zkt
$ dnssec-signer -N /etc/named.conf
```

- Simple configuration file (extract of `dnssec.conf`)

```
# zone specific timing values
ResignInterval: 3d      # (259200 seconds)
Sigvalidity:    30d     # (2592000 seconds)
Max_TTL:        6h      # (21600 seconds)
Propagation:    5m      # (300 seconds)

# signing key parameters
KSK_lifetime:   0
KSK_algo:       DSA     # (Algorithm ID 3)
KSK_bits:       1024
ZSK_lifetime:   10d     # (864000 seconds)
ZSK_algo:       RSASHA1 # (Algorithm ID 5)
ZSK_bits:       512
```

- Full automatic ZSK rollover (pre-publish key algorithm)
- Automatic serial number incrementation  
Supports sequential serial number and `YYYYmmDDxx` format

## ZKT – Configuration

- Create a directory for each secure zone (dirname = domainname)

```
$ mkdir example.net.  
$ cd example.net.
```

- Create the zone file (default name: zone.db)

```
$ head -15 zone.db  
$TTL 7200  
; Be sure that the serial number below is left  
; justified in a field of at least 10 spaces!!  
; 0123456789;  
@ IN SOA ns1.example.net. hostmaster.example.net. (  
        63          ; Serial  
        43200       ; Refresh  
        1800        ; Retry  
        2W          ; Expire  
        7200 )      ; Minimum  
  
        IN NS ns1.example.net.  
        IN NS ns2.example.net.  
  
$INCLUDE dnskey.db           ;include the DNSKEY records  
...
```

## ZKT – Configuration(2)

- Create a (just empty) zone.db.signed file

```
$ touch zone.db.signed
$ ls -l
-rw-r----- 1 dnsop dnsop 916 2005-08-14 13:54 zone.db
-rw-r--r-- 1 dnsop dnsop 0 2005-08-14 13:55 zone.db.signed
```

- Sign the zone

```
$ dnssec-signer -v -o example.net.
parsing zone "example.net." in dir "."
    No active KSK found: generate new one
    No active ZSK found: generate new one
    Re-signing necessary: Modified keys
    Writing key file "./dnskey.db"
    Incrementing serial number (64) in file "./zone.db"
    Signing zone "example.net."

$ ls -l
-rw-r--r-- 1 dnsop dnsop 581 2005-08-14 13:55 Kexample.net.+003+18710.key
-rw----- 1 dnsop dnsop 688 2005-08-14 13:55 Kexample.net.+003+18710.private
-rw-r--r-- 1 dnsop dnsop 121 2005-08-14 13:55 Kexample.net.+005+57705.key
-rw----- 1 dnsop dnsop 545 2005-08-14 13:55 Kexample.net.+005+57705.private
-rw-r--r-- 1 dnsop dnsop 1136 2005-08-14 13:55 dnskey.db
-rw-r--r-- 1 dnsop dnsop 71 2005-08-14 13:55 dsset-example.net.
-rw-r--r-- 1 dnsop dnsop 702 2005-08-14 13:55 keyset-example.net.
-rw-r----- 1 dnsop dnsop 916 2005-08-14 13:55 zone.db
-rw-r--r-- 1 dnsop dnsop 4080 2005-08-14 13:55 zone.db.signed
```

## ZKT – Configuration(3)

- Show current key status

```
$ dnssec-zkt -a .
```

Keyname	Tag	Typ	Sta	Algorit	Generation	Time	Age
example.net.	18710	KSK	act	DSA	Aug 14 2005	13:55:24	13m42s
example.net.	57705	ZSK	act	RSASHA1	Aug 14 2005	13:55:24	13m42s

- Change the zonefile in named.conf

```
zone "example.net." in {  
    type master;  
    file "example.net./zone.db.signed";  
};
```

- Force re-signing and reload the zone

```
$ dnssec-signer -r -f -v -N named.conf  
parsing zone "example.net." in dir "./."  
Re-signing necessary: Option -f  
Writing key file "././dnskey.db"  
Incrementing serial number (65) in file "././zone.db"  
Signing zone "example.net."  
Reload zone "example.net."
```

- Check messages in /var/log/named

```
14-Aug-2005 14:34:43.198 general: info: zone example.net/IN: loaded serial 65 (signed)
```

## ZKT – Configuration(4)

- Periodic re-sign your zone  
Call `dnssec-signer` at least once a day

- cron is your friend

```
$ crontab -l
21 6 * * * /home/dnsop/dnssec-cron 2>&1 | logger -t dnssec-cron -p daemon.info
21 18 * * * /home/dnsop/dnssec-cron 2>&1 | logger -t dnssec-cron -p daemon.info
```

- The `dnssec-cron` script looks simple

```
echo "current zone signing keys"
/home/dnsop/bin/dnssec-zkt -z
echo "dnssec re-signing process started"
/home/dnsop/bin/dnssec-signer -v -v -r -N /var/named/named.conf
```

- Create the trusted-keys Section for your resolver configuration

```
$ dnssec-zkt -T -l example.net.
trusted-keys {
"example.net."      257 3 3 "CJEUcyN1ES5bAnBI40+m7nLhbmTfxVtF3104agNve+6Hu8kZ8EKzm+/U
                    +qh2NXv6+UgowadnPlfHHwLzpfNP4aZXfXa2qog1P5dp7POUquW6zn25
                    ...
                    Wdlf/F/2lJh2LF4bU616EyOeRichLvlBXn15nkkLr4usbPitr68DrVas
                    o6bci4LJlPJBkHVS/3MtBo0lSY3XvoiBJtgp" ; # key id = 18710
};
```

## Summary

- BIND-Tools are good for basic zone signing and key generation
- Additional tools available
  - For key management
  - For automatic zone signing
- Some DNSSEC secured zones found „in the wild“
  - .se
  - All RIPE reverse zones (.in-addr.arpa, .ip6.arpa)
  - Currently round about 450 .de-Domains secured
- What next?
  - Standards and tools for DS registration and key rollover
  - Secure (stub) resolver librarys (some implementations available)
  - Tools for resolver management (SEP-Management)
  - More secure TLDs! (.de, .arpa, .com, .net, .org, .eu)

## References

Olaf Kolkman, Ripe-NCC DISI

„DNSSEC Howto Version 1.5“

([http://www.ripe.net/disi/dnssec\\_howto/dnssec\\_howto.pdf](http://www.ripe.net/disi/dnssec_howto/dnssec_howto.pdf))

Nominum

BIND v9 Administrator Reference Manual

BIND v9 Administrator Reference Manual

(<http://www.nominum.org/content/documents/bind9arm.pdf>)

RFCs 4033 (DNS Security Introduction and Requirements)  
4034 (Resource Records for the DNS Security Extensions)  
4035 (Protocol Modifications for the DNS Security Extensions)

Drafts DNSSEC Operational Practices  
draft-ietf-dnsop-dnssec-operational-practices-06.txt

Links <http://www.dnssec.net>  
<http://secspider.cs.ucla.edu/secspider/>  
<http://www.iks-jena.de/leistungen/dnssec/>  
<http://www.hznet.de/dns/dnssec-denic040929.pdf>  
<http://www.hznet.de/zkt/>

# Questions ?

# Questions ?

*<http://www.hznet.de/dns/dnssec-denic060404en.pdf>*

## Questions ?

*<http://www.hznet.de/dns/dnssec-denic060404en.pdf>*

Thank you  
for your attention!

CONTENTS

..... 1

DNSsec or ..... How 1

DNSsec Practice (Bind Tools) ..... 3

DNSsec Practice (2) ..... 4

Key Rollover ..... 5

DNSsec Tools ..... 6

DNSsec Tools (2) ..... 7

Zone Key Tool (ZKT) ..... 8

ZKT – Configuration ..... 9

ZKT – Configuration(2) ..... 10

ZKT – Configuration(3) ..... 11

ZKT – Configuration(4) ..... 12

Summary ..... 13

References ..... 14

..... 15