Experience from a Swedish Agency and a Nordic operator

fredrik@xpd.se

Overview

- Skatteverket (Swedish Tax Agency)
  - End user perspective
- TDC
  - Registrar perspective

Skatteverket

- Why DNSSEC?
- How to deploy?
  - What tools?
- How to maintain?
- Pros and Cons
- Costs

Why?

Swedish Tax Agency

- Be able to trust DNS information
  - This really is www.skatteverket.se
- Prevent some types of DNS attacks
  - Kaminsky comes to mind :P
- Secure SMTP TLS encryption

Why?

- Foundation for SPF and DKIM/ADSP
- Future use
  - SSHFP (RFC4255) and IPSECKEY (RFC4025) DNS RR

How?

- Lots of reading and pestering DNSSEC gurus with tons of idiotic questions :)
- First tests was done on a non-production zone (skv.se) in 2008
- Manual use of BIND9 tools
- Use the .SE DomainManager for DS verification

How?

Swedish Tax Agency

- Maintaining the keys is cumbersome
- So is zone signing..
- .. and key rollover
  - for both ZSK and KSK
- not to mention incrementing SOA serial number :-)

Keys

- KSK (Key Signing Key)
  - Lifetime of 1 year (2 year)
- ZSK (Zone Signing Key)
  - Lifetime of 1 month

ZKT

- Meet ZKT (Zone Key Tool) by Holger Zuleger
- Very easy to setup and maintain
- Automatic ZSK rollover
- Automatic resigning of the zone
  - Including incrementing SOA serial :P

ZKT

- Create zone.db and zone.db.signed
  - Add $INCLUDE dnskey.db to zone.db
- Sign the zone with dnssec-signer
  - Generates ZSK and KSK
- Update named.conf

ZKT

- Add trust anchor for the new zone
- Add a cron(1) entry to call dnssec-signer a couple of times per day

ZKT


```
$ cat zone.db
$TTL 1d
@           IN      SOA     a.dns.tdc.se. fredrik.xpd.se. (
            2009110201  ; serial  [yyyyMMddNN]
                    24H ; refresh [6h]
                    2H  ; retry   [2h]
                    4W  ; expire  [8d]
                    1H) ; minimum [1d]

            IN      NS      a.dns.tdc.se.
            IN      NS      b.dns.tdc.se.
            IN      NS      c.dns.tdc.se.

   3600     IN      A       213.131.154.136

$include dnskey.db
```

ZKT


```
$ dnssec-signer -v -o test.se.
parsing zone "test.se." in dir "."
        Check RFC5011 status
        Check KSK status
        No active KSK found: generate new one
        Check ZSK status
        No active ZSK found: generate new one
        Re-signing necessary: Modfied zone key set
        Writing key file "./dnskey.db"
        Incrementing serial number in file "./zone.db"
        Signing zone "test.se."
        Signing completed after 0s.
```

ZKT


```
$ dnssec-zkt -t
Keyname                   Tag Typ Sta Algorit                 Age
        test.se. 49327 KSK act RSASHA1                   2m45s
        test.se. 17691 ZSK act RSASHA1                   2m45s

$ crontab -l
25 06,18 * * * /usr/local/lbin/dnssec-cron 2>&1 | /usr/bin/
logger -t dnssec-cron -p daemon.info
```

Production

- Production on skatteverket.se zone went live in mid January 2009
  - To not interfere with any year end jobs
- Use the .SE DomainManager for DS verification

Tools

- ZKT (Zone Key Tool) as described earlier
- chkexp
  - Checks enddate on SMTP TLS certificates
  - Checks signatures on DNSSEC signed zones
  - Alerts via mail or SNMPv3

chkexp

- DNSSEC code based on the checkexpire.pl script from NLnet Labs
  - Utilizes the perl module NET::DNS::SEC
- SMTP TLS check is wrapper around OpenSSL

chkexp


```
$ chkexp -v
Running test "/opt/chkexp/bin/dnssec-chkexp -v --warn=24 skatteverket.se" -- passed
skatteverket.se is delegated to dns5.telia.com (81.228.11.68)
skatteverket.se is delegated to b.dns.songnetworks.se (213.50.29.195)
skatteverket.se is delegated to ystad.dns.swip.net (192.71.220.12)
skatteverket.se is delegated to a.dns.songnetworks.se (213.50.29.190)
81.228.11.68: zone "skatteverket.se" verified with signature made with key 47418.
81.228.11.68: Signature will expire within 219 hours
213.50.29.195: zone "skatteverket.se" verified with signature made with key 47418.
213.50.29.195: Signature will expire within 219 hours
192.71.220.12: zone "skatteverket.se" verified with signature made with key 47418.
192.71.220.12: Signature will expire within 219 hours
213.50.29.190: zone "skatteverket.se" verified with signature made with key 47418.
213.50.29.190: Signature will expire within 219 hours
```

Maintenance

Swedish Tax Agency

- Yearly
  - Update chosen trust anchors
- Daily
  - Check signatures on zones

Remember

Swedish Tax Agency

- Change authentication mechanism for zone transfers to any secondary
  - Create TSIG keys for each partner
  - and distribute safely (PGP)
- Don’t forget to backup KSK and ZSK regulary and in a safe manner

Pros and Cons

- Cons
  - DNS just went from forget in the closet to need of maintenance
  - More complicated (troubleshooting et al)

Initial costs

Swedish Tax Agency

- Roughly 80 hours from first test to production
  - Tests with DNSSEC and tools
  - External contacts (Slaves, .SE)
    - Setup AXFR with TSIG securely (PGP)
    - Operational documentation

Yearly costs

- Yearly maintenance
  - Estimated at 40 hours per year

Skatteverket

Questions?

TDC

- Nordic operator covering Sweden, Denmark, Norway and Finland
- TDC fiberoptic network covers more than 80% of all Nordic companies with more than 10 employees.

TDC

- TDC is the second largest supplier on the IP-VPN market in Sweden, and as the third largest ISP for the Swedish commercial company market.

TDC

- Why DNSSEC?
- How to deploy DNSSEC?
- What tools are used?

Why?

- Need to be able to provide DNSSEC support to it's customer base
- Two perspectives:
  - Being a resolver operator
  - Authoritative name server operator

Why?

- Customer demand
- Be part of the solution, not the problem

How?

- Roughly 5000 zones
- Initial effort was entirely ZKT based
  - On a PTS grant
  - Worked flawless

How?

- Old environment w/o DNSSEC support needs to be phased out
  - Analysis of query logs from old resolvers
  - Move zones from old environment to new

Tools

- Uses a mix of Open source software to implement DNSSEC able resolvers and authoritative name servers
- To get some resilience to software bugs and misconfigurations

Tools

- Linux
- Hardened Ubuntu 9.10 Server
- Custom Debian packages for ease of maintenance

Tools

- BIND9
  - Internet Systems Consortium
  - “BIND .. is a reference implementation of those protocols (DNS), but it is also production-grade software, suitable for use in high-volume and high-reliability applications.”

Tools

- NSD3
  - NLnet Labs
  - “NSD is an authoritative only, high performance, simple and open source name server”

Tools

- Unbound
  - NLnet Labs, Kirei, Verisign and Nominet
  - “Unbound is a validating, recursive, and caching DNS resolver”

OpenDNSSEC

- .SE (The Internet Infrastructure Foundation), NLNetLabs, Nominet, Kirei, SURFnet, SIDN and John Dickinson.
- ”OpenDNSSEC was created as an open-source turn-key solution for DNSSEC. It secures zone data just before it is published in an authoritative name server.”

OpenDNSSEC

- Will start using version 0 (svn)
- Will migrate to version 1.x.x in 2010
- Hopefully OpenDNSSEC will be apt-get'able then.

TDC

Questions?