DNSSEC – implementation & test

Internetdagarna 2006

Uppdrag till Netlight från PTS

- Testa följande
  - Implementation av DNSSEC
    - Zonsignering och lokal aktivering (i master)
    - Förtroendekedja från .se
    - Aktivering i resolver
  - Administration och funktionalitet
    - Zon-ägaren
    - Resolver
    - Slutanvändare

Implementationsförfarande DNSSEC

1. Säkerställande av namnserver-version
2. Lokal signering av zon
3. Införskaffande av klientcertifikat
4. Registrering av certifikat i KEYMAN (https://keyman.nic.se/)
5. Undertecknande av testavtal till .SE
6. Avvakta verifiering och godkännande av certifikat från .SE
7. Aktivera förtroendekedja från .SE

Implementation DNSSEC, – steg 1

Säkerställande av namnserver-version

- BIND 9.3.x eller senare: full funktionalitet
- Microsoft DNS mycket begränsad funktionalitet
  - Ej signera eller verifiera zon-information
  - Ej agera säkerhetsmedveten resolver (validera DNSSEC records)

  = ej användbart i detta sammanhang

Implementation DNSSEC, steg 2

- Lokal signering av zon
  - Aktivera DNSSEC, genom *dnssec-enable yes* i named.conf
  - Generera nyckelpar (*dnssec-keygen*)
    - Zone-signing key (ZSK)
    - Key-signing key (KSK)
  - Signera zon (*dnssec-signzone*)
  - Konfigurera named.conf att läsa in den signerade zon-filen

- Fungerar mycket bra
- Grafiska verktyg finns, men även lätt vid manuell process

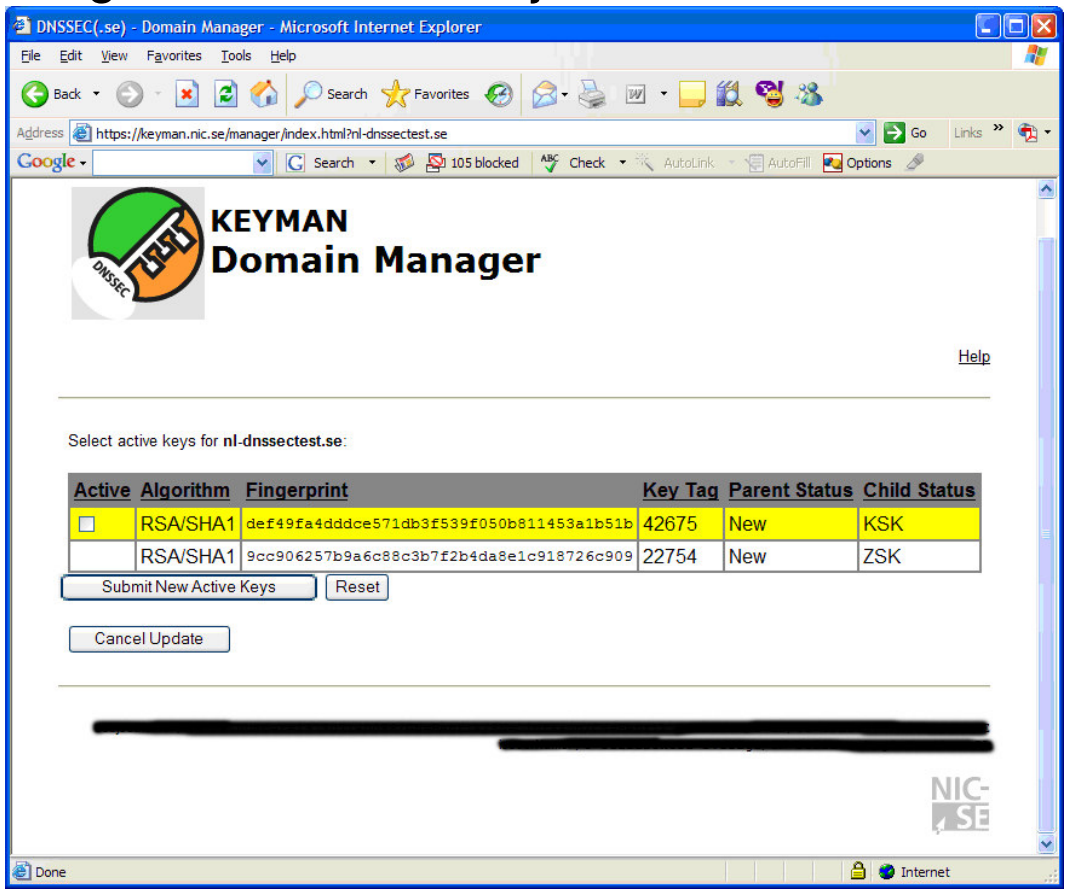
Implementation DNSSEC, steg 3-6

- Registrering hos .SE
  - Klientcertifikat (e-legitimation) krävs
  - Uppladdning av certifikat till KEYMAN
    - Koppling av certifikat mot domän
  - Testavtal och godkännande av detta
    - Aktivering av domän-administration

- Bra dokumentation och presentation!
  - http://dnssec.iis.se/
- Processen tog ca en vecka

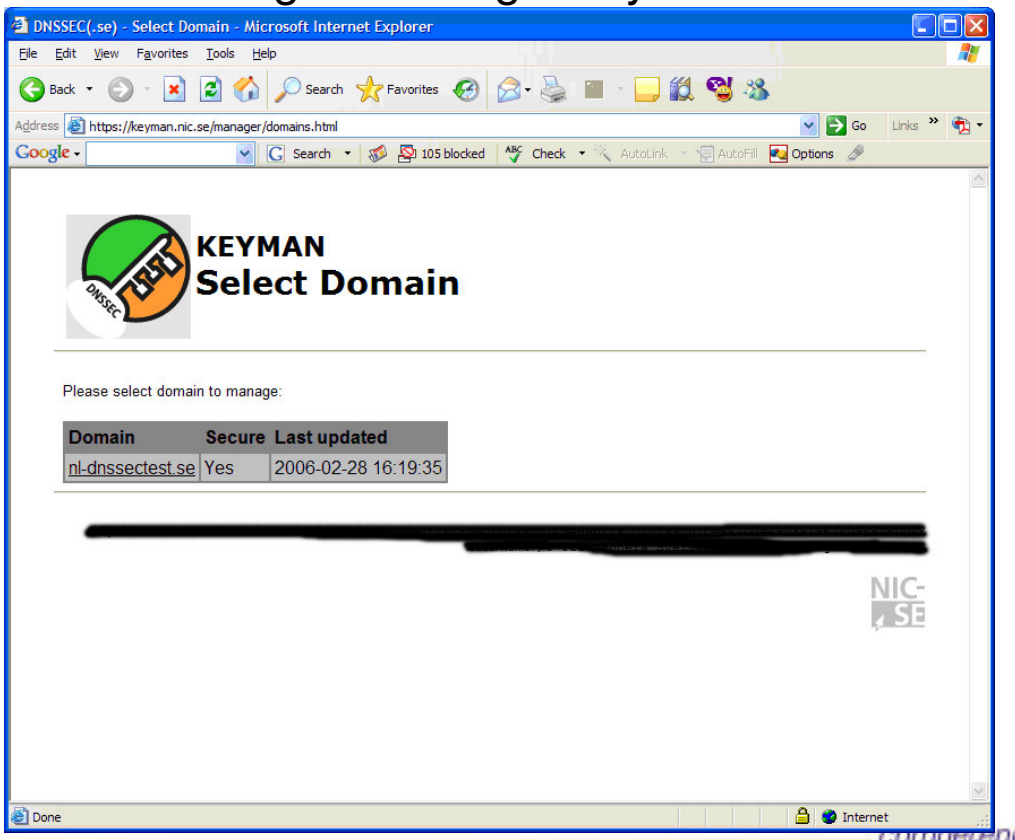
Implementation DNSSEC, steg 7

- Aktivering av förtroendekedja från .se - KEYMAN



Implementation DNSSEC, steg 7

- KEYMAN (https://keyman.nic.se/)
  - Enkel administration av förtroendekedja
  - Automatisk inhämtning/verifiering av nyckel-information från zonfil



Administration DNSSEC, 1/2

Två tillägg till normal DNS-administration:

- Omsignering av zonen
  - Vid uppdatering av zoninformation
  - Då RRSIG går ut (ca 30 dagar)

- Byte av nycklar
  - ZSK: förpubliceringsmetoden
  - KSK: dubbelsignatursmetoden

Administration DNSSEC, 2/2

- Omsignering av zoninformation
  - Mycket lätt och snabbt
  - Går att automatisera ganska lätt
- Byte av nycklar
  - Fler-stegs-process
  - Administration både på namnserver och i KEYMAN
  - Kräver god ordning och dokumentation – dock ej svårt
  - Dagens grafiska verktyg saknar stöd för detta

Testutförande, 1/2

Testmiljö

- Master-DNS för zon nl.dnssectest.se (BIND 9.3.x)
- Epost- och webbserver för nl-dnssectest.se
- DNSSEC-medvetna resolvers (BIND 9.3.x + MS DNS)

I alla testfall testades två saker:

- Access till en på servern liggande webbsida, http://www.nl-dnssectest.se/
- Att skicka e-post till test@nl-dnssectest.se

I alla testfall kontrollerades följande saker:

- Resultatet för användaren, dvs. kom vi fram till rätt webbsida och kom e-posten fram?
- Loggutskrift på resolver-DNS
- Loggutskrift på master-DNS

Testutförande, 2/2

Tre scenarion

- Utan förtroendekedja från .se till nl-dnssectest.se
- Med förtroendekedja från .se till nl-dnssectest.se
- Byte av nycklar (med förtroendekedja)

Testvariabler (där användbart)

- *Trusted keys* inlagda i named.conf på resolver:
  - Inga trusted keys
  - korrekt .se nyckel
  - felaktig .se nyckel
  - korrekt nl-dnssectest.se nyckel
  - felaktig nl-dnssectest.se nyckel
- Övriga variabler:
  - cache/no-cache i resolver
  - *dnssec-must-be-secur*e på/av för domän nl-dnssectest.se i resolver
  - hackat zon-record i nl-dnssectest.se master-DNS
    - ersätt IP med den för www.pts.se
  - felaktig nyckel till nl-dnssectest.se hos .se
    - helt ny zonsignering
    - key rollover
  - korrekt, men ny, nyckel till nl-dnssectest.se hos .se

Testresultat

- Dålig kommunikation till slutanvändaren
- Hantering av cache och loggning oklar
- Man är alltid beroende av att den som *frågar* använder DNSSEC

- Felaktiga/utdaterade nycklar ger stora konsekvenser
  - Felaktig nyckel till .se hos resolver gör alla .se-domäner otillgängliga
  - Ett par specialfall gav oväntat resultat

  = god koll på administration av nycklar krävs hos 3:e part (resolver) som vill använda DNSSEC

Slutsats

- DNSSEC är enkelt att implementera och, för den som är van DNS-administratör, hyfsat enkel att administrera
  - KEYMAN bra verkyg för administration av förtroendekedja från .se
  - God information på http://dnssec.iis.se/
  - BIND 9.3.x eller likvärdig krävs
  - Automatiserade verktyg för administration behövs dock
- Avsaknad av fullt stöd i Microsoft DNS ett avbräck
- Informationen kring DNSSEC och de effekter som uppstår vid ett felaktigt DNSSEC-svar obefintliga för både slutanvändaren och administratören av DNS-beroende applikationer (t.ex. e-post)
- DNSSEC känns därför i dagsläget enbart praktiskt användbar för de aktörer som är verksamma på de högre nivåerna i DNS-hierarkin, t.ex. toppdomäner och ISP:er.

Hela rapporten: http://www.pts.se/

Frågor kring implementation och test:

Henrik Olofsson, Netlight Consulting AB
henrik.olofsson@netlight.se
0735-418111