
# .SE

# Signerad sedan 2005

## Hur känns det 12 månader senare?

**Anne-Marie Eklund Löwinder, amel@iis.se**

**Jakob Schlyter, jakob@kirei.se**

# Vad är .SE?

- ISO 3166-1 Alpha 2-kodelement för konungariket Sverige
- TLD administreras och drivs av en stiftelse
  - Drygt 500 000 registrerade domännamn
  - En daglig tillväxt med ~500 domäner
  - Driften starkt diversifierad och baserad på:
    - Unicast och Anycast
    - Geografisk spridning
    - Olika arkitektur, plattformar och DNS-programvaror

# .SE (Stiftelsen för Internetinfrastruktur)

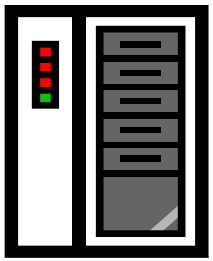
- .SE (Stiftelsen för Internetinfrastruktur) ansvarar för Internets svenska toppdomän, .SE.
- Kärnverksamheten är registrering av domännamn samt administration och teknisk drift av det nationella domännamnsregistret under .SE.
- .SE är en oberoende allmännyttig organisation som verkar för en positiv utveckling av Internet i Sverige. Stiftelsen avsätter varje år medel till projekt som på olika sätt bidrar till Internets utveckling och användning.

# Vad gör DNS för dig?

Berättar för maskiner vart de ska vända sig när du:

- Skriver en webbadress
- Skickar e-post

***Användare***



***ISP***

***Namnserver-operatör***

Cache

Resolver

Namnserver

Har jag redan svaret?
- Skicka det till resolvern

Om inte, kontakta namnserver

Är jag uppkopplad?
Vart ska jag för att få reda på svaret?
- Min lokala ISP

Hitta IP-adressen
Skicka tillbaka den

# Var kan det bli fel?

- Förfalskning – DNS-data som kommer som svar till den lokala ISP:n kan vara förfalskat. Särskilt enkelt på ett trådlöst nätverk. Resultat: Du hamnar där du inte hade den minsta avsikt att hamna.

- Förvanskning – DNS-data kan modifieras. Orsakar den lokala ISP:ns cache att ha giltig men felaktig information om vart du ska ta vägen.

- Avlyssning – Någon avlyssnar DNS-data innan det skickas vidare.

- Annat som kan gå fel - Förändring av zondata - Icke-auktoriserade uppdateringar

# Vad är DNSSEC?

- DNSSEC är Internets svar på identitetsstölder i DNS
  - Det skyddar användare från och låter systemen upptäcka DNS-attacker
- I princip allt i DNSSEC signeras digitalt
  - Tillåter autentisering av KÄLLAN till DNS-data
  - Garanterar INTEGRITET I DNS-data
- Om DNS-data MODIFIERAS, förstörs eller på annat sätt kompromettеras under transport…
  - Då är signaturen inte längre verifierbar och därmed inte heller giltig

# Varför vill vi ha DNSSEC i .SE?

- Ökar integriteten i DNS.
- Ökar säkerheten för .SE:s domäninnehavare och deras användare.
  - En åtgärd mot pharming och andra DNS MITM attacker.
  - Förstärker infrastrukturen för Internet.
  - En tänkbar användning av DNSSEC är dessutom för säker distribution av attribut för andra säkerhetsprotokoll och lösningar.
- Efterfrågas av ansvarig myndighet, PTS.
- Behövs för att kunna lita på nya kritiska applikationer
  - t.ex. ENUM

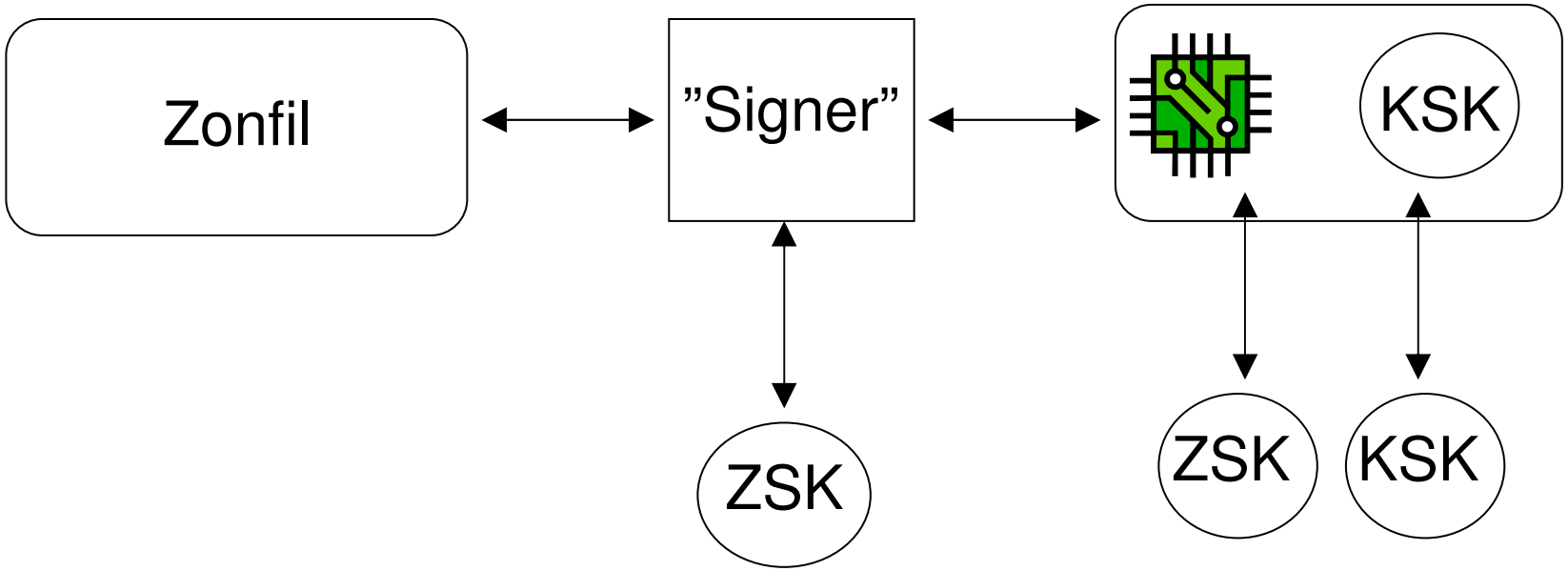
# När?

- Den första workshopen ägde rum i februari 1999
- Tester har pågått sedan januari 2003
- Öppna tester sedan januari 2004
- RFC 4033, 4034 & 4035 (DNSSEC bis) publicerades i mars 2005.
- .se började distribuera den signerade .se-zonen den 13 september 2005.
- .se började ta emot signerade delegeringar från tidiga användare från mitten av november 2005.
- Mer omfattande testverksamhet inleddes februari 2006.
- Kommersiellt tillgängligt Q1 2007?

Vad har vi lärt oss?

En hel del!

# Nyckeladministration är kritiskt



# Övervakning är viktigt

- Nagios har utökats för att utföra basala DNSSEC-kontroller:
  - Varnar för signaturer som är på väg att gå ut
  - Testar den extra DNSSEC-hanteringen i produktionen så att den görs korrekt
  - Kontrollerar äktheten hos vissa signaturer

# Det här sa vi redan förra året…

- Använd inte BIND 8
- Förvissa er om att brandväggarna klarar EDNS
- Separera rekursiva och auktoritativa namnservrar
- Operatörer: Lär er hur det fungerar
- Kunder: Ställ krav på att det finns

# Var tar DNSSEC mer resurser?

- Zonhantering
  - Tid för signering
  - Ökad storlek på zonfilerna
- Auktoritära nameservers
  - Ökad storlek på zonfilerna
  - Prestanda
  - Bandbredd
- Rekursiva nameservers
  - Prestanda
  - Bandbredd

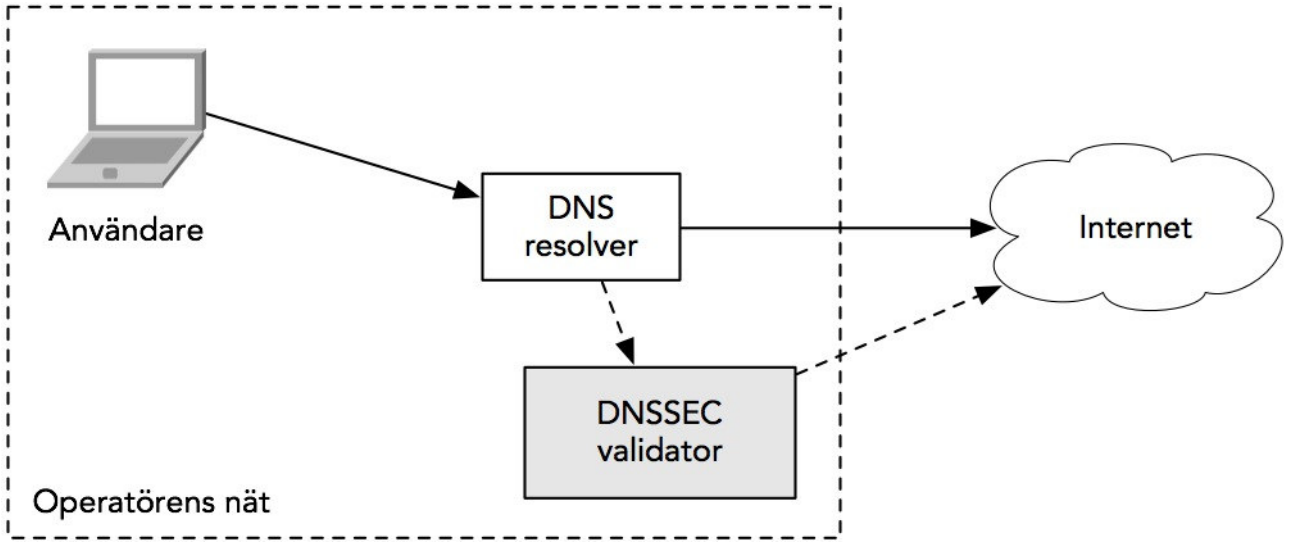
# Validering hos Internetoperatörerna

- Vi tror att det är bra om Internetoperatörernas rekursiva namnservrar gör validering.
- Hur visar vi att det fungerar och vad som krävs?
- Blir det någon större prestandaförändring?
  - Bandbredd
  - Svarstider
  - Felfrekvens

# Idé

- Slå på validering hos en stor operatör
- … men …
- Gör det försiktigt

# Testuppsättning



# Tidplan

- PTS gör tester tillsammans med en eller flera operatörer under vintern.
- Testrapport klar under början av våren.

Tack så mycket!

?